#2
Drueth
5-28-01

PRICE AND GESS

JOSEPH W. PRICE
ALBIN H. GESS
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE
J. RONALD RICHEBOURG

OF COUNSEL
JAMES F. KIRK

ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pg@pgpatentlaw.com

PRIORITY DOCUMENT
(Japan 2000-085133)

Inventor(s): Seiichiro Tamai

Title: **AN APPARATUS FOR IDENTITY VERIFICATION, A SYSTEM FOR IDENTITY VERIFICATION, A CARD FOR IDENTITY VERIFICATION AND A METHOD FOR IDENTITY VERIFICATION, BASED ON IDENTIFICATION BY BIOMETRICS**

Attorney's Docket No.: NAK1-BO25

EXPRESS MAIL LABEL NO. EL 852658608 US

DATE OF DEPOSIT: March 19, 2001

J.W. PRICE 949/261.5433
Seiichiro TAMAI
NAKJ-B025

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ３月２４日

出 願 番 号
Application Number: 特願２０００－０８５１３３

出 願 人
Applicant (s): 松下電子工業株式会社

２０００年１１月１７日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０９５０４７

【書類名】　特許願

【整理番号】　2925010112

【提出日】　平成12年 3月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/64

【発明者】

【住所又は居所】　大阪府高槻市幸町１番１号　松下電子工業株式会社内

【氏名】　玉井　誠一郎

【特許出願人】

【識別番号】　000005843

【氏名又は名称】　松下電子工業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【選任した代理人】

【識別番号】　100109210

【弁理士】

【氏名又は名称】　新居　広守

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9810106

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　バイオメトリックに基づく本人認証装置、本人認証システム、本人認証用カード及び本人認証方法

【特許請求の範囲】

【請求項１】　バイオメトリックに基づいて本人認証を行う装置であって、

非接触で身体の部位を撮影することによりバイオメトリック画像を取得する撮影手段と、

取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、予め登録されたバイオメトリック情報と照合することにより、本人認証を行う認証手段と

を備えることを特徴とする本人認証装置。

【請求項２】　前記本人認証装置は、さらに、適正な撮影位置で前記部位が撮影されるように前記撮影手段による撮影の方向と倍率とを制御する撮影制御手段を備える

ことを特徴とする請求項１記載の本人認証装置。

【請求項３】　前記本人認証装置は、さらに、前記部位又は前記部位を含むより大きな部位を繰り返して撮影するように前記撮影手段を制御し、得られた複数の画像に基づいて、身体の動きを検出する動き検出手段を備え、

前記認証手段は、前記動き検出手段によって身体の動きが検出され、かつ、前記部位が適正な撮影位置で撮影されたと判断された場合に、本人認証を行う

ことを特徴とする請求項１記載の本人認証装置。

【請求項４】　前記部位は、虹彩であり、

前記動き検出手段は、前記虹彩に光を照射するとともに、その照射に同期して

虹彩を撮影するように前記撮影手段を制御する

ことを特徴とする請求項３記載の本人認証装置。

【請求項５】　前記本人認証装置は、さらに、繰り返して前記部位を撮影するように前記撮影手段を制御する繰り返し制御手段を備え、

前記認証手段は、繰り返し撮影によって得られた複数のバイオメトリック画像に基づいて前記バイオメトリック情報を抽出し、本人認証を行う

ことを特徴とする請求項１記載の本人認証装置。

【請求項６】　前記本人認証装置は、さらに、身体の複数の部位について、前記バイオメトリック画像を取得し、取得されたバイオメトリック画像を表示し、前記ガイド画像を表示し、前記部位が適正な撮影位置で撮影されたか否かを判断するように前記撮影手段と、前記バイオメトリック画像表示手段と、前記ガイド表示手段と、判断手段とを制御する複数部位制御手段を備え、

前記認証手段は、取得された複数の部位のバイオメトリック画像から複数の部位についてのバイオメトリック情報を抽出し、それらバイオメトリック情報の組み合わせと予め登録された対応するバイオメトリック情報の組み合わせとを照合することにより、本人認証を行う

ことを特徴とする請求項１記載の本人認証装置。

【請求項７】　前記認証手段は、前記複数の部位ごとの照合結果を示す一致度それぞれに異なる重みづけをした後に加算して得られる総合評価値が一定のしきい値を超えるか否かによって、前記本人認証を行う

ことを特徴とする請求項６記載の本人認証装置。

【請求項８】　前記複数の部位は、指紋と虹彩であることを特徴とする請求項６記載の本人認証装置。

【請求項９】　前記複数の部位は、異なる指の指紋であることを特徴とする請求項６記載の本人認証装置。

【請求項１０】　前記複数の部位は、両目の虹彩であることを特徴とする請求項６記載の本人認証装置。

【請求項１１】　前記本人認証装置は、さらに、前記撮影に伴って、本人の識別に役立つ情報であるＩＤデータを取得するＩＤデータ取得手段を備え、

前記認証装置は、前記バイオメトリック情報及び前記ＩＤデータの組み合わせと予め登録されたバイオメトリック情報及びＩＤデータの組み合わせとを照合することにより、本人認証を行う

ことを特徴とする請求項１記載の本人認証装置。

【請求項１２】　前記認証手段は、予め登録された複数のバイオメトリック情報の中から、ＩＤデータが一致するものを特定し、特定したバイオメトリック情報と抽出された前記バイオメトリック情報との同一性によって、本人認証を行う

ことを特徴とする請求項１１記載の本人認証装置。

【請求項１３】　前記認証装置は、さらに、

予め登録された前記バイオメトリック情報を記憶する記憶手段と、

前記記憶手段に記憶されたバイオメトリック情報を前記認証手段により抽出されたバイオメトリック情報で置き換える登録情報更新手段を備える

を備えることを特徴とする請求項１記載の本人認証装置。

【請求項１４】　前記更新手段は、予め定められた一定期間を超えてバイオメトリック情報が更新されていない場合に、前記バイオメトリック情報を置き換える

ことを特徴とする請求項１３記載の本人認証装置。

【請求項１５】　通信ネットワークを介して接続された認証端末と認証サーバとからなるバイオメトリックに基づく本人認証システムであって、

前記認証端末は、

非接触で身体の部位を撮影することによりバイオメトリック画像を取得する撮影手段と、

取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、前記認証サーバに送信するバイオメトリック情報抽出手段とを備え、

前記認証サーバは、

予め登録された複数のバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、

前記認証端末から送信されてきたバイオメトリック情報と前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報とを照合することにより、本人認証を行う認証手段とを備える

ことを特徴とする本人認証システム。

【請求項１６】　前記認証端末は、さらに、

前記撮影に伴って、本人の識別に役立つ情報であるＩＤデータを取得するＩＤデータ取得手段と、

取得されたＩＤデータを認証サーバに送信することにより、そのＩＤデータと一致するＩＤデータに対応するバイオメトリック情報を前記認証サーバからダウンロードするダウンロード手段と、

ダウンロードされたバイオメトリック情報と前記バイオメトリック情報抽出手段により抽出されたバイオメトリック情報とを照合することにより、本人認証を行う認証手段とを備え、

前記認証サーバは、さらに、

前記バイオメトリック情報記憶手段に記憶された複数のバイオメトリック情報それぞれに対応するＩＤデータを予め記憶するＩＤデータ記憶手段と、

前記バイオメトリック情報記憶手段及び前記ＩＤデータ記憶手段を参照することにより、前記認証端末から送信されたきたＩＤデータと一致するＩＤデータに対応するバイオメトリック情報を読み出して前記認証端末に送信するバイオメトリック情報送信手段とを備える

ことを特徴とする請求項１５記載の本人認証システム。

【請求項１７】　バイオメトリックに基づく本人認証に用いられる携帯型のカードであって、

身体の部位の形態的な特徴を示すバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、

身体の部位を示す画像データを外部から取得する画像データ取得手段と、

取得された画像データからバイオメトリック情報を抽出し、前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報と照合することにより、本人認証を行う認証手段と

を備えることを特徴とする本人認証用カード。

【請求項１８】　請求項１記載の本人認証装置が組み込まれた携帯電話機。

【請求項１９】　請求項１記載の本人認証装置が組み込まれたパーソナルコンピュータ。

【請求項２０】　ビルディングへの人の出入りを管理するビル管理システムであって、

請求項１記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、前記ビルディングに出入りするための扉を開錠する制御手段と

を備えることを特徴とするビル管理システム。

【請求項２１】　請求項１記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、エンジン始動を許可する制御手段と

を備えることを特徴とする自動車。

【請求項２２】　請求項１記載の本人認証装置と、

前記認証装置により本人認証が成功した場合に、指定された商品を取り出し口に移動させる制御手段と

を備えることを特徴とする自動販売機。

【請求項２３】　請求項１記載の本人認証装置と、

前記認証装置による本人認証の結果に応じて入出金処理を行う入出金処理手段と

を備えることを特徴とする現金自動預払機。

【請求項２４】　請求項１記載の本人認証装置と、

前記認証装置による本人認証の結果に応じて入出金処理を行う入出金処理手段と

を備えるＰＯＳ端末装置。

【請求項２５】　通信ネットワークを介して接続された認証端末と認証サーバとから構成され、バイオメトリックに基づく本人認証による電子決済を行うためのシステムであって、

前記認証端末は、

操作者から電子決済を行いたい旨の要求を受け付ける受付手段と、

非接触で前記操作者の身体の部位を撮影することによりバイオメトリック画像を取得する撮影手段と、

取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、前記電子決済を特定する情報とともに前記認証サーバに送信するバイオメトリック情報抽出手段とを備え、

前記認証サーバは、

予め登録された複数のバイオメトリック情報を記憶するバイオメトリック情報記憶手段と、

前記認証端末から送信されてきたバイオメトリック情報と前記バイオメトリック情報記憶手段に記憶されたバイオメトリック情報とを照合することにより、本人認証を行う認証手段と、

本人認証に成功したときに、前記認証端末から送られてきた情報によって特定される電子決済を行う決済手段とを備える

ことを特徴とする電子決済システム。

【請求項２６】　バイオメトリックに基づいて本人認証を行う方法であって、

非接触で身体の部位を撮影する撮影手段を制御することによりバイオメトリック画像を取得する撮影ステップと、

取得されたバイオメトリック画像を表示手段に表示するバイオメトリック画像表示ステップと、

適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて前記表示手段に表示するガイド表示ステップと、

前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断ステップと、

適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、予め登録されたバイオメトリック情報と照合することにより、本人認証を行う認証ステップと

を含むことを特徴とする本人認証方法。

【請求項２７】　バイオメトリックに基づいて本人認証を行うためのプログラムが記録されたコンピュータ読み取り可能な記録媒体であって、

前記プログラムは、請求項２６記載のステップをコンピュータに実行させることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、バイオメトリックに基づいて本人認証を行う装置、その装置を利用して金融・流通等の決済を行うシステム、そのための携帯型カード及び本人認証方法等に関する。

【０００２】

【従来の技術】

電子商取引やカード決済等においては、パスワードや署名等によって本人認証

が行われる。ところが、これらパスワードや署名は、盗聴や偽造、なりすまし等の不正行為による攻撃を受け易い。そのために、最近では、より高いセキュリティを維持するために、バイオメトリック（生体測定）に基づく本人認証が行われている。その代表的なものに、バイオメトリックセンサによって指紋の画像を取得し、予め登録しておいた指紋画像と照合することによって生体を識別し、本人認証を行う認証装置がある（特開２０００－３００２８号公報の「認証装置」等）。

【０００３】

図１８は、従来の認証装置が備えるバイオメトリックセンサの例を示す。図１８（ａ）は、光学式指紋スキャナと呼ばれる方式であり、プリズム等のガラス面に押圧された指の指紋をＣＣＤ等を用いてスキャンすることで、光学的に指紋画像を読み取る方式である。図１８（ｂ）は、静電容量型指紋センサチップによる方式であり、コンデンサアレイが形成された半導体センサの表面に指が置かれたときの各コンデンサの静電容量を検出することにより指紋画像を読み取る方式である。

【０００４】

このようにして読み取った指紋画像と予め登録しておいた指紋画像とを照合することにより本人認証が行われている。

【０００５】

【発明が解決しようとする課題】

ところが、上記のようなバイオメトリックセンサによる従来の認証装置は、以下の問題を有している。

（１）ガラス面に指を接触させて指紋の画像を取得する方式に起因する以下の問題がある。

【０００６】

つまり、繰り返し使用によってガラス面が汚れるので、定期的にガラス面をクリーニングする等の保守が必要とされる。また、静電気が生じ易いこと、及び、指の押圧がかかること等を考慮すると、上述の半導体センサは十分に実用に耐え得るとは言えない。さらに、他人が触れたガラス面に触りたくないという嫌悪感

をいだくユーザを考慮する必要もある。

（２）指紋の読取専用のバイオメトリックセンサを備える必要があるために、装置全体がコスト高となってしまう。

（３）指紋だけを用いて本人認証をしていることに基づく以下の問題がある。

【０００７】

つまり、指に包帯を巻いていたり、火傷や擦り切れたために指紋を採取することが困難なユーザに対しては、もはや本人認証を実施することができない。また、指紋画像を用いた認証の精度が必ずしも十分に高いとは言えない。

そこで、本発明は、かかる問題点に鑑みてなされたものであり、バイオメトリックセンサの保守がほとんど不要であり、静電気や押圧に対する問題を生じることがなく、かつ、ユーザに心理的な不快感や嫌悪感を与えることなくバイオメトリック画像を取得して本人認証を行う認証装置等を提供することを第１の目的とする。

【０００８】

また、低コストで、かつ、精度の高い本人認証を行う認証装置等を提供することを第２の目的とする。

【０００９】

【課題を解決するための手段】

上記第１の目的を達成するために、本発明に係る認証装置等は、ビデオカメラを用いて、非接触でバイオメトリック画像を取り込むことを特徴とする。そのために、認証装置は、表示画面を有し、その表示画面に、カメラが撮影している画像と適正な撮影位置を示すガイド画像とを表示する。ユーザは、認証装置の表示画面に映し出された自分の指とガイド画像とが重なるように、指の位置を移動させればよい。これによって、非接触センシングによる鮮明なバイオメトリック画像の取り込みが実現され、接触センシングに起因する従来の問題が解消される。

【００１０】

また、上記第２の目的を達成するために、本発明に係る認証装置が備えるカメラは、指紋だけでなく、虹彩（アイリス）、掌形、顔形等の複数のバイオメトリック画像を取り込み、それら画像による複数の識別結果を組み合わせて本人認証

を行う。これによって、認証精度が向上されるとともに、異なる種別のバイオメトリック画像それぞれを取得するための複数のセンサを備える場合に比べ、極めて低コストによる本人認証が実現される。

【００１１】

また、取得したバイオメトリック画像と照合する基準データ（予め登録されたバイオメトリック情報）については、一定期間ごと、又は、ユーザからバイオメトリック画像を取得する度に、最新の内容に更新していく。これによって、基準データが最新のものに維持され、高い精度による本人認証が維持される。

また、取得したバイオメトリック画像と基準データとの照合において、バイオメトリック画像だけでなく、ユーザから取得した名前や生年月日等のＩＤデータを組み合わせて照合する。例えば、照合の対象となる個人データの候補をＩＤデータによって絞り込んでおいた後に、バイオメトリック画像に基づく照合を行う。これによって、本人認証の精度が向上されるとともに、本人認証に要する時間が短縮される。

【００１２】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

図１は、本発明に係る電子マネーシステム１０の全体構成を示す図である。この電子マネーシステム１０は、バイオメトリックに基づく本人認証によって消費者が電子決済を行うことが可能なシステムであり、インタネット等の通信ネットワーク２０を介して接続された認証サーバ３０、ゲートウェイ４０、携帯電話機５０、ＰＤＡ（Personal Digital Assistance；携帯情報端末）６０、ＡＴＭ（Automated Teller Machine；現金自動預払機）７０、ＰＣ（Personal Computer）８０、銀行用通信端末９０及び電子ショップ用通信端末１００等から構成される。

【００１３】

この電子マネーシステム１０においては、消費者のバイオメトリック画像（ここでは、少なくとも指紋及び虹彩のいずれかの画像）は、各通信装置５０、６０、７０及び８０が備えるカメラによって非接触に取得され、本人認証のための必

須の情報となっている。一方、ＩＤカード１１０は、バイオメトリック画像に基づく本人認証を補助するために用いられる。

【００１４】

認証サーバ３０は、携帯電話機５０、ＰＤＡ６０及びＰＣ８０から送られてくる特徴データ（バイオメトリック画像から抽出された指紋又は虹彩の特徴を示すデータ）を受信し、予めデータベースとして登録された特徴データと照合することによって本人認証を行い、その結果を取引先の電子ショップや銀行に報告する等の決済処理等を集中的に実行するコンピュータである。

【００１５】

ここで、認証サーバ３０に備えられているデータベースは、図２に示されるように、この電子マネーシステム１０を利用する全ての会員（消費者）について、ＰＩＣ（Personal Identification Code；個人識別コード）、ＩＤデータ（ＩＤカード１１０に記録されている個人識別情報）、その会員のバイオメトリック画像、そのバイオメトリック画像から抽出された特徴データ、それらバイオメトリック画像及び特徴データが登録された年月日等を対応づけて集めたものである。なお、この電子マネーシステム１０では、本人認証の精度を確保するために、バイオメトリック画像と特徴データのうち、少なくとも２つの特徴データが登録されていることが条件とされる。

【００１６】

この認証サーバ３０は、ＡＴＭ７０等から、特徴データを参照したい旨の要求をＩＤデータと共に受け取った場合には、そのＩＤデータが一致する特徴データをデータベース中で検索し、該当する全ての特徴データを読み出して暗号化した後にＡＴＭ７０等の要求元に返信するというデータ配信機能も有する。

さらに、この認証サーバ３０は、本人認証に成功し、かつ、その本人についての特徴データが一定期間（例えば、３年）を超えて更新されていない場合は、携帯電話機５０等から送られてきた最新の特徴データで古い特徴データを置き換えることにより、データベースを更新したり、この電子マネーシステム１０の新規会員に対してＩＤカード１１０を発行する機能も有する。

【００１７】

銀行用通信端末９０は、銀行に設置されたコンピュータであり、消費者、認証サーバ３０及びＡＴＭ７０等からの通信による決済の指示に従って、入出金や振替等の金融処理を行う。

電子ショップ用通信端末１００は、ネットワーク上で商品を販売する販売主が所有するコンピュータであり、消費者、認証サーバ３０等からの注文指示等を受けて販売処理を行う。

【００１８】

ゲートウェイ４０は、携帯電話機５０やＰＤＡ６０等による無線電話網と通信ネットワーク２０とを接続する無線基地局等である。

携帯電話機５０及びＰＤＡ６０は、それぞれ、一般的な携帯電話機及び携帯情報端末としての機能に加えて、内蔵する小型カメラにより、操作者のバイオメトリック画像を取得し、その画像から特徴データを生成して認証サーバ３０に送信することによって、その場での電子決済を可能とする移動端末としての機能を有する。操作者は、カードを用いたり、パスワードを入力したりすることなく、携帯電話機５０及びＰＤＡ６０の表示画面と対話するだけで、希望商品を注文する等の商取引を行うことができる。

【００１９】

ＡＴＭ７０は、一般的な現金自動預払機の機能に加えて、ビデオカメラにより、操作者のバイオメトリック画像を取得し、その画像又はその画像とＩＤカード１１０から読み出したＩＤデータとに基づいて、認証サーバ３０と通信しながら、又は、認証サーバ３０と通信することなく（スタンドアローンで）、本人認証を遂行し、その結果に応じて入出金処理を行う機能を有する。

【００２０】

つまり、操作者は、ＩＤカード１１０を所持している場合にはＡＴＭ７０にそのＩＤカード１１０を挿入した後に本人認証を終えることで、また、ＩＤカード１１０を所持していない場合であっても本人認証を終えることで、パスワード等を入力することなく、自分の口座からお金を引き出したりすることができる。

ＰＣ８０は、オフィスや家庭に設置されるコンピュータであり、一般的なコンピュータとしての機能に加えて、上記ＰＤＡ６０が有する機能や、自分のＩＤカ

ード１１０に記録されている特徴データを更新する等の機能を有する。操作者は、このＰＣ８０の表示画面と対話することで、希望商品を注文したり、ＩＤカード１１０の内容を書き換えることによる保守をしたりすることができる。

【００２１】

図３（ａ）～（ｃ）は、この電子マネーシステム１０で用いられるＩＤカード１１０の種別を示す図である。ここには、３種類のＩＤカード１１０ａ～ｃが示されている。

図３（ａ）に示されたＩＤカード１１０ｂは、最も簡易なタイプ１のＩＤカードであり、表面に磁気ストライプや光学メモリが形成されたプラスチックカードである。これら磁気ストライプや光学メモリには、持主のＩＤデータ（名前、生年月日、住所、電話番号、パスワード）が記録されている。これらＩＤデータは、例えば、ＡＴＭ７０により本人認証が行われる際に、照合対象となる特徴データを認証サーバ３０中で検索するときの検索キーとして用いられる。

【００２２】

図３（ｂ）に示されたＩＤカード１１０ｂは、上記ＩＤカード１１０ａによる磁気メモリ又は光学メモリに加えて、表面に電極を露出させた不揮発なＩＣメモリ（フラッシュメモリ）を内蔵している。このＩＣメモリには、持主の特徴データが記録される。この特徴データは、例えば、ＡＴＭ７０によるその場での本人認証、即ち、そのＩＤカード１１０ｂの使用者と持主との同一性を判断する等のための用いられる。具体的には、ＡＴＭ７０のカメラを介して取得された使用者の特徴データとＡＴＭ７０に挿入されたＩＤカード１１０ｂに記録されていた特徴データとの同一性が判断される。

【００２３】

図３（ｃ）に示されたＩＤカード１１０ｃは、最も高機能なＩＤカードであり、上記ＩＤカード１１０ｂに備えられている磁気又は光学メモリ及びＩＣメモリに加えて、本人認証を自ら実行するための認証回路を内蔵している。このＩＤカード１１０ｃは、認証処理を実行するためのプログラムを格納したＲＯＭ及びそのプログラムを実行するＣＰＵ等からなる回路を備え、ＡＴＭ７０やＰＣ８０のカメラを介して取得された特徴データと内部のＩＣメモリに記録されている特徴

データとの同一性を自ら判断する。従って、このＩＤカード１１０ｃが用いられた場合には、認証サーバ３０やＡＴＭ７０での認証処理は不要となる。

【００２４】

図４は、図１に示されたＡＴＭ７０が備える認証装置２００、即ち、ＡＴＭ７０のうち本発明に係る本人認証に関連する部分の構成を示すブロック図である。なお、携帯電話機５０、ＰＤＡ６０、ＰＣ８０及び認証サーバ３０についても、この認証装置２００と同一の構成又はそのサブセット（一部の構成）が内蔵されている。

【００２５】

この認証装置２００は、操作者と対話しながら非接触でバイオメトリック画像を取得し、その画像から特徴データを抽出した後に、認証サーバ３０やＩＤカード１１０に登録された特徴データと照合することにより、本人認証を実行する（又は、認証サーバ３０やＩＤカード１１０ｃに実行させる）装置であり、撮影条件切替部２１０、リーダライタ部２２０、通信Ｉ／Ｆ（Interface）部２３０、カメラ部２４０、画像処理部２５０、制御部２６０、画像表示部２７０、入力部２８０、暗号部２８５及びメモリ部２９０から構成される。

【００２６】

カメラ部２４０は、本人認証に用いられる身体の部位（ここでは、指紋及び虹彩）を撮影し、カラーの画像信号を出力する小型ビデオカメラ等である。

図５は、カメラ部２４０の詳細な構成を示すブロック図である。このカメラ部２４０は、Ｚ駆動部２４３、撮像レンズ２４４、イメージセンサ部２４５及びＡＦ制御部２４６からなる可動のアセンブリである可動部２４１と、θ駆動部２４２と、キャプチャ制御部２４７と、発光部２４８とから構成される。

【００２７】

撮像レンズ２４４は、広角のズームレンズである。

Ｚ駆動部２４３は、撮像レンズ２４４をＺ方向（遠近方向）に駆動するアクチュエータ等であり、撮影条件切替部２１０からの指示に基づいて撮像レンズ２４４をズーミングすることにより、撮影倍率を変化させたり、ＡＦ制御部２４６からの指示に基づいて撮像レンズ２４４をＺ方向に微小移動させることにより、フ

ォーカシングを行う。

【００２８】

ＡＦ制御部２４６は、発光部２４８等から発せられた光の反射光をイメージセンサ部２４５等で検出させることによって、被写体までの距離を計測し、その距離に応じてＺ駆動部２４３を制御する自動焦点調整回路である。

イメージセンサ部２４５は、例えば、３５０×４００画素のＣＭＯＳイメージセンサ等からなる撮像素子である。なお、ＣＭＯＳイメージセンサは、ＣＰＵ等の回路と一体化させることが容易であり、低消費電力である点で、このイメージセンサ部２４５の材料として好ましい。

【００２９】

θ駆動部２４２は、撮影条件切替部２１０からの指示に基づいて、ジャイロ機構等により可動部２４１を２次元的に回転（地面に水平及び垂直方向に回転）させるアクチュエータ等である。

発光部２４８は、自動焦点調整及びストロボ用の光を発光するＬＥＤやフラッシュ回路等である。

【００３０】

キャプチャ制御部２４７は、撮影条件切替部２１０からの指示に基づいて、イメージセンサ部２４５に対して画像をサンプリングする（カラーイメージを保持する）旨の指示を出したり、発光部２４８に対してストロボ発光等を指示したりする。発光部２４８にストロボ発光を指示したときには、このキャプチャ制御部２４７は、ストロボ発光と同期させて（被写体の瞳孔が小さくなった瞬間に）画像をサンプリングするようイメージセンサ部２４５に指示を出す。

【００３１】

撮影条件切替部２１０は、制御部２６０から、撮像条件（段階的に設定された複数の撮影倍率の１つ及び複数の撮影方向の１つ）や微調整のための指示を受け取り、その条件や指示に対応する制御信号をカメラ部２４０のＺ駆動部２４３及びθ駆動部２４２に送ることによって、カメラ部２４０の撮影倍率と撮影方向を粗く変化させたり、微調整したりする。これによって、カメラ部２４０による被写体（操作者の身体部位）の追尾制御が行われ、イメージセンサ部２４５上の予

め定められた最適位置に最適なサイズでバイオメトリック画像が結像される。

【００３２】

また、撮影条件切替部２１０は、制御部２６０から虹彩を撮影する旨の指示を受けた場合には、キャプチャ制御部２４７に対して、上述のようなストロボ発光と同期した撮影（以下、「ストロボ同期撮影」という。）を行うように指示する。これは、照度が十分でない場所においても、瞳孔を絞り込んだ状態での虹彩、即ち、大きな面積を有する虹彩の撮影と可能としたり、生体が生きていることの確認をしたりするためである。

【００３３】

なお、携帯電話機５０及びＰＤＡ６０に装備される認証装置は、ＡＴＭ７０に装備される認証装置２００とは異なり、カメラ部２４０のＺ駆動部２４３及び撮影条件切替部２１０を備えておらず、固定化された撮影倍率と撮影方向で被写体を撮影する（ただし、ＡＦ制御部２４６による自動焦点調整及びキャプチャ制御部２４７によるストロボ同期撮影は行われる）。

【００３４】

つまり、携帯電話機５０及びＰＤＡ６０に装備される認証装置は、予め定められた適正な空間位置に被写体が置かれることを前提としている。ただし、そのような適正位置に被写体を誘導するために、画像表示部２７０にガイド画像（被写体の適正な撮影位置を示す画像）を表示する。

画像処理部２５０は、ＡＤ変換器、バッファメモリ、デジタルフィルタ（スムージング、エッジ検出、特徴抽出用フィルタ）及び演算器等からなり、制御部２６０からの指示に従って、カメラ部２４０のイメージセンサ部２４５から送られてきたカラー画像の信号をデジタル化し、得られたバイオメトリック画像のデータに対して必要なフィルタリング処理等を行うことで被写体の輪郭や特徴を抽出する。

【００３５】

つまり、画像処理部２５０は、制御部２６０からの要求に従って、(i)カメラ部２４０により撮影されたカラー画像の全て（バイオメトリック画像の全体）、(ii)指又は目の輪郭位置を示す輪郭データ、(iii)その輪郭に囲まれた部分の画

像（切り出されたバイオメトリック画像）、及び、(iv)指紋の特徴点等を特定するデータ（指紋の特徴データ）又は虹彩の特徴を示すアイリスコード（虹彩の特徴データ）のいずれかを生成し、制御部２６０に渡す。

【００３６】

図６は、画像処理部２５０が生成する指紋の特徴データを説明するための図である。特徴データは、指紋の特徴点（分岐点及び端点）や中心点の相対位置、隆線の位置及び方向が数値化されたものである。

図７は、画像処理部２５０が生成する虹彩の特徴データを説明するための図である。虹彩とは、黒目の内側で瞳孔より外側のドーナツ状の部分をいい、瞳孔の開き具合を調節する筋肉から構成される。虹彩の特徴データは、虹彩の中心を原点とする極座標において半径方向と回転方向とに予め分割された複数の領域それぞれにおけるアイリスパターン（放射状に描かれる虹彩のパターン）の濃淡を示す２値データが符号化されたもの（２５６バイトのアイリスコード等）である。

【００３７】

リーダライタ部２２０は、３種類のＩＤカード１１０ａ～ｃに対応した記録再生装置であり、装着されたＩＤカード１１０に記録されたＩＤデータ及び特徴データを読み出したり、ＩＤカード１１０に特徴データを書き込んだりする。

通信Ｉ／Ｆ部２３０は、モデムカード、ＬＡＮカード及び無線による送受信回路等であり、ゲートウェイ４０や通信ネットワーク２０等を介してこの認証装置２００が認証サーバ３０等と通信するためのインタフェース回路である。

【００３８】

画像表示部２７０は、携帯電話機５０等が備えるカラーＬＣＤやＡＴＭ７０等が備えるカラーＣＲＴ等であり、本認証装置２００においては、本人認証の際に操作者の指や目を適正な撮影位置に誘導する際のガイド表示等のために用いられる。

入力部２８０は、携帯電話機５０等が備えるキーやＡＴＭ７０等が備えるタッチスパネル等であり、本認証装置２００においては、操作者が、認証装置２００との対話したり、バイオメトリックに基づく本人認証を補助するためのＩＤデータを入力したりする際に用いられる。

【００３９】

暗号部２８５は、この認証装置２００が通信Ｉ／Ｆ部２３０を介して本人認証に関わるデータ（バイオメトリック画像、特徴データ、ＩＤデータ等）を外部装置（認証サーバ３０等）に送信する際に、チャレンジレスポンスによる機器間の相互認証を行うとともに時変の秘密鍵を共有化しあい、その秘密鍵によって送信データを事前に暗号化したり、相互認証の後で外部装置から送信されてきた暗号データに対して秘密鍵を用いて復号化したりする回路である。

【００４０】

メモリ部２９０は、不揮発性のＩＣメモリ等からなる基準データ格納部２９１及びプログラム格納部２９２と、揮発性のＩＣメモリ等からなる一時データ格納部２９３から構成される。

基準データ格納部２９１は、一般的な人の指（左右の手それぞれの親指、人差指）及び目（右目と左目）の輪郭（形状）を示す輪郭基準データ２９１ａを予め格納している。この輪郭基準データ２９１ａは、この認証装置２００が本人認証に用いられる被写体の指又は目の位置を認識するために用いられる。

【００４１】

プログラム格納部２９２は、(i)鮮明なバイオメトリック画像を取得する等のための制御手順を記述した画像取得プログラム２９２ａと、(ii)取得された特徴データと、認証サーバ３０やＩＤカード１１０に登録されている特徴データとの照合手順を記述した照合プログラム２９２ｂと、(iii)その他の付加的な処理（登録、照合テスト、撮影条件の設定等）手順を記述したユーティリティプログラム２９２ｃとを予め格納している。

【００４２】

一時データ格納部２９３は、比較対象となる特徴データ２９３ａやＩＤデータ２９３ｂ等を一時的に格納する作業領域である。

制御部２６０は、携帯電話機５０やＡＴＭ７０等が備えるＣＰＵ、ＲＡＭ及びカレンダ・タイマ回路等からなり、操作者が電子決済をしようとして認証サーバ３０等から身元確認をすべき旨の指示を受けたり、操作者からの指示を受けたりしたときに、プログラム格納部２９２に格納されている対応するプログラム２９

２ａ～ｃを実行する。これによって、この認証装置２００は、それを備える各通信装置５０、６０、７０及び８０の種別等に応じて、以下の機能を発揮する。

（１）バイオメトリック画像の取得

具体的には、(i)ガイド画像の表示によるバイオメトリック画像の取得（携帯電話機５０及びＰＤＡ６０の場合）と、(ii)追尾制御によるバイオメトリック画像の取得（ＡＴＭ７０やＰＣ８０の場合）がある。

（２）照合による本人認証

具体的には、(i)認証サーバ３０への委託による認証（携帯電話機５０、ＰＤＡ６０、ＡＴＭ７０及びＰＣ８０の場合）と、(ii)ＩＤカード１１０への委託による認証（ＡＴＭ７０及びＰＣ８０の場合）と、(iii)自ら実行することによる認証（ＡＴＭ７０の場合）がある。

（３）ユーティリティ処理

具体的には、(i)認証サーバ３０又はＩＤカード１１０への特徴データの登録と（ＡＴＭ７０及びＰＣ８０の場合）、(ii)登録された特徴データをテストするための照合テスト（全ての通信装置５０、６０、７０及び８０が対象）と、(iii)撮影条件の設定（全ての通信装置５０、６０、７０及び８０が対象）がある。

【００４３】

次に以上のように構成された電子マネーシステム１０の動作について、認証装置２００の動作を中心に説明する。

図８は、本認証装置２００によるバイオメトリック画像の取得における基本的な動作（通常モード）の手順を示すフローチャートである。なお、本人認証に用いられるバイオメトリック画像の種類（指紋画像のみ、虹彩画像のみ、指紋画像と虹彩画像との組み合わせ等）は、認証サーバ３０から認証装置２００への通知等によって事前に決定され、制御部２６０の内部メモリに記憶されている。

【００４４】

まず、制御部２６０は、操作者による指示等に基づいて、本人認証に用いられる身体部位（例えば、右手親指）を特定した後に、その身体部位に対応する輪郭基準データ２９１ａを基準データ格納部２９１から読み出し、その輪郭基準データ２９１ａが示す輪郭を赤い線図（ガイド画像）として画像表示部２７０に表示

する（ステップＳ３００）。

【００４５】

そして、制御部２６０は、キャプチャする旨の指示が操作者から発せられるか、又は、１秒等の一定時間が経過するまで、カメラ部２４０の撮影倍率及び撮影方向の調整による被写体の追尾制御と（ステップＳ３０１）、画像処理部２５０によるバイオメトリック画像の取得及び画像表示部２７０への表示(ステップＳ３０２）とを、繰り返す（ステップＳ３０３）。

【００４６】

具体的には、制御部２６０は、撮影条件切替部２１０に対して、身体部位の種類に対応して予め設定されている撮影条件等を送ることによって、カメラ部２４０のＺ駆動部２４３やθ駆動部２４２やキャプチャ制御部２４７を作動させた後に、画像処理部２５０によるデジタル化によって得られたバイオメトリック画像を取得し、その画像を画像表示部２７０にカラーで表示出力する。なお、本人認証に用いられる身体部位の種類に応じて、撮影のための適正位置が予め操作者に知らされている。例えば、指であれば、カメラ部２４０の撮像レンズ２４４から５ｃｍだけ手前の位置、目であれば、３０ｃｍだけ手前の位置等である。

【００４７】

このような身体部位の動画表示とガイド表示によって、操作者は、画像表示部２７０に表示されたガイド画像と自分の親指の輪郭とがピッタリと重なり合うように、指や携帯電話機５０等を動かして位置調整することができる。そして、適正位置になったと判断したときに、入力部２８０のボタン等によってキャプチャ指示を発することができる。

【００４８】

操作者からキャプチャ指示が発せられるか、又は、１秒等の一定時間が経過すると（ステップＳ３０３でＹｅｓ）、制御部２６０は、上記更新表示（ステップＳ３０１～Ｓ３０３）を中断し、直前に取得されたバイオメトリック画像を画像表示部２７０に静止画として表示出力するとともに（ステップＳ３０４）、得られたバイオメトリック画像が適正位置で撮影されたものか否かを判断する（ステップＳ３０５～Ｓ３０６）。

【００４９】

具体的には、制御部２６０は、画像処理部２５０に指示することにより、直前に取得されたバイオメトリック画像から右手親指の輪郭を抽出させ（ステップＳ３０５）、その輪郭と輪郭基準データ２９１ａが示す輪郭との一致度（相関値）を算出し、一定の基準値以上であるか否か判断する（ステップＳ３０６）。例えば、エッジ検出と２値化等によって、輪郭部分の画素ブロックだけ“１”となる輪郭データを生成し、２つの輪郭データにおける同一位置の画素値どうしの排他的論理和をとり、その結果が“１”となる（画素値が一致する）画素の数を一致度とし、基準値と比較する。

【００５０】

その結果、一致度が基準値未満である場合には（ステップＳ３０６でＮｏ）、制御部２６０は、それら２つの輪郭について、スケール（撮影倍率）のずれと方向（撮影方向）のずれとを算出し、その結果を撮影条件切替部２１０に指示することにより、再び、ガイド表示（ステップＳ３０１～Ｓ３０３）と輪郭の一致度の判定（ステップＳ３０４～Ｓ３０６）とを繰り返す。

【００５１】

一方、一致度が基準値以上である場合には（ステップＳ３０６でＹｅｓ）、制御部２６０は、画像処理部２５０に指示することにより、バイオメトリック画像を切り出した後に指紋の特徴データを抽出させ、その結果（切り出されたバイオメトリック画像と特徴データ）を取得し、一時データ格納部２９３に格納する（ステップＳ３０７）。

【００５２】

このようにして、認証装置２００は、ガイド表示によって、操作者の身体部位を適正な撮影位置に誘導し、身体と接触することなく、予定された大きさと鮮明度のバイオメトリック画像及び特徴データを取得することができる。

図９は、高精度モードにおける本認証装置２００によるバイオメトリック画像の取得動作の手順を示すフローチャートである。ここで、高精度モードとは、図８に示された取得手順を繰り返す等によってバイオメトリック画像（及び特徴データ）を高精度に取得するオプション的な動作モードであり、操作者から入力部

２８０を介して予め指示される。

【００５３】

このモードにおいては、認証装置２００は、バイオメトリック画像の取得（ステップＳ３１３～Ｓ３１６）に先立ち、生体が生きていることを確認する（ステップＳ３１０～Ｓ３１２）。これは、死んでいる生体を用いた不正な本人認証を防止する等のためである。

具体的には、制御部２６０は、撮影条件切替部２１０に指示を出すことにより、（１）ストロボ同期撮影と通常撮影それぞれにおける虹彩画像を取得し、瞳孔の拡大や収縮の有無を検出したり、（２）手や顔全体の撮影を一定時間間隔で繰り返し、得られた画像から抽出した輪郭を比較することにより、生体の動きを検出したりする（ステップＳ３１０）。その結果、動きが検出されなかった場合には（ステップＳ３１１でＮｏ）、以降の処理を中止し（ステップＳ３１２）。

【００５４】

動きが検出された場合には（ステップＳ３１１）、予め定められた回数ｎだけ、バイオメトリック画像の取得と特徴データの抽出を繰り返す（ステップＳ３１３～Ｓ３１６）。具体的には、制御部２６０は、図８に示される手順を繰り返す。ただし、上記動き検出において、手や顔全体の動きを検出した場合には（ステップＳ３１０）、制御部２６０は、その手又は顔全体の位置を用いて局部（身体部位）の位置を決定し、その身体部位に焦点を合わせるようにカメラ部２４０のＺ駆動部２４３及びθ駆動部２４２を制御する。

【００５５】

このようにしてｎセットの特徴データが得られると、制御部２６０は、それら特徴データを平均化することにより、最終的な特徴データとして生成する（ステップＳ３１７）。具体的には、指紋の同一特徴点を示す位置座標を平均化したり、アイリスパターンの濃淡値を合計した後に２値化してアイリスコードを生成したりする。

【００５６】

このようにして、高精度モードによるバイオメトリック画像によれば、時間的な変化画像の平均化により、図８に示された通常モードにおける場合に比べ、撮

影に要する時間は少し長くなるものの、生きた生体に対する本人認証が行われ、より高いセキュリティに対応した本人認証が可能となる。

図１０は、本認証装置２００による特徴データの照合における全体的な流れを示すフローチャートである。つまり、本図には、図８や図９に示された手順によって操作者の特徴データ（及びＩＤデータ）が取得された後における認証装置２００の動作手順が示されている。

【００５７】

まず、制御部２６０は、リーダライタ部２２０からの信号に基づいて、ＩＤカード１１０が装着されているか否か（ステップＳ３２０）、及び、装着されている場合には、そのＩＤカード１１０のタイプ１～３を検出する（ステップＳ３２１）。

その結果、タイプ１のＩＤカード１１０ａが装着されている場合には（ステップＳ３２１でタイプ１）、制御部２６０は、一時データ格納部２９３に格納されている操作者のＩＤデータ２９３ｂを読み出して暗号部２８５に暗号化させた後に、通信Ｉ／Ｆ部２３０を介して認証サーバ３０に送信する（ステップＳ３２５）。このときに、送信したＩＤデータを検索キーとし、その内容に一致する全ての特徴データを返信させる旨の命令も併せて送る。

【００５８】

そして、認証サーバ３０から返信されてきた１以上の特徴データを受け取ると、制御部２６０は、それら受信した特徴データ全てを対象として、既に取得している操作者の特徴データと逐次比較していくことで、一致度を算出する（ステップＳ３２６）。その結果、一定のしきい値を超える一致度の特徴データが１つ以上発見された場合には、その操作者を本人と認証し、そうでなければ認証を否定する（ステップＳ３３０）。

【００５９】

一方、タイプ２のＩＤカード１１０ｂが装着されている場合には（ステップＳ３２１でタイプ２）、制御部２６０は、リーダライタ部２２０を介してそのＩＤカード１１０ｂから特徴データを読み出し（ステップＳ３２４）、その特徴データを認証基準として、上記と同様の照合（ステップＳ３２６）と認証（ステップ

Ｓ３３０）を行う。

【００６０】

また、タイプ３のＩＤカード１１０ｃが装着されている場合には（ステップＳ３２１でタイプ３）、一時データ格納部２９３に格納されている操作者の特徴データ２９３ａを読み出し、その特徴データと照合させる命令とをリーダライタ部２２０を介してＩＤカード１１０ｃに送ることで（ステップＳ３２２）、ＩＤカード１１０ｃに照合を実行させる（ステップＳ３２３）。そして、ＩＤカード１１０ｃによる照合の結果（一致度）を受け取ると、制御部２６０は、その照合結果に基づく認証を行う（ステップＳ３３０）。

【００６１】

一方、ＩＤカード１１０が装着されていない場合には（ステップＳ３２０でＮＯ）、制御部２６０は、その旨を画像表示部２７０に表示し、それに対して操作者が入力部２８０を介してＩＤデータを入力してきたか否か判断する（ステップＳ３２７）。

その結果、操作者がＩＤデータを手動で入力してきた場合には（ステップＳ３２７でＹｅｓ）、制御部２６０は、そのＩＤデータを、タイプ１のＩＤカード１１０ａから読み出したＩＤデータと同様の取り扱いをする（ステップＳ３２５～Ｓ３３０）。

【００６２】

一方、操作者がＩＤデータの入力を拒否した場合には（ステップＳ３２７でＮｏ）、制御部２６０は、一時データ格納部２９３に格納されている操作者の特徴データ２９３ａを読み出し、照合させるための命令と共に認証サーバ３０に送ることで（ステップＳ３２８）、認証サーバ３０に対して特徴データだけによる照合を実行させる（ステップＳ３２９）。そして、認証サーバ３０による照合の結果（一致度）を受け取ると、制御部２６０は、その照合結果に基づく認証を行う（ステップＳ３３０）。

【００６３】

このようにして、認証装置２００は、特徴データに基づく本人認証を行うが、ＩＤデータを利用することができる場合には、そのＩＤデータを本人認証の補助

（検索の高速化）として利用する。また、様々な環境に応じて、認証サーバ３０、認証装置２００及びＩＤカード１１０のいずれかにおいて照合処理が行われ、本人認証に伴う処理負荷の分散が図られる。

【００６４】

図１１は、図１０における照合（ステップＳ３２３、Ｓ３２６及びＳ３２９）及び認証（ステップＳ３３０）の詳細な手順、即ち、認証装置２００の制御部２６０、タイプ３のＩＤカード１１０ｃの認証回路及び認証サーバ３０により実行される照合及び認証処理の詳細な手順を示すフローチャートである。ここでは、認証装置２００の制御部２６０が指紋と虹彩との組み合わせによる照合と認証を行う場合を説明する。

【００６５】

制御部２６０は、カメラ部２４０等を制御することにより、図８に示された手順に従って、操作者の指紋の特徴データを取得するとともに、予め登録された基準となる指紋の特徴データを認証サーバ３０から通信Ｉ／Ｆ部２３０を介して取得し、一時データ格納部２９３に格納する（ステップＳ３４０）。そして、それら指紋の特徴データどうしを照合し、その一致度Ｃ１を算出する（ステップＳ３４１）。例えば、両特徴データそれぞれに含まれる複数の指紋の特徴点のうち、一定範囲内で相対位置が一致する特徴点の個数の割合等を一致度Ｃ１として算出する。

【００６６】

同様にして、制御部２６０は、操作者の虹彩の特徴データと、登録された基準となる虹彩の特徴データとを取得して一時データ格納部２９３に格納し（ステップＳ３４２）、それら特徴データどうしを照合し、その一致度Ｃ２を算出する（ステップＳ３４３）。例えば、両特徴データそれぞれに含まれるアイリスコードにおけるハミング距離を求め、それに対応する「確からしさ」の確率を一致度Ｃ２として算出する。

【００６７】

そして、制御部２６０は、得られた２つの一致度Ｃ１及びＣ２それぞれに対して、予め設定された重み係数ｋ１及びｋ２を乗じて加算することで総合評価値を

出し、その総合評価値が一定のしきい値以上であるか否か判断し（ステップＳ３４４）、総合評価値がしきい値以上である場合には（ステップＳ３４４でＹｅｓ）、本人認証を肯定し（ステップＳ３４５）、そうでない場合には（ステップＳ３４４でＮｏ）、本人認証を否定する（ステップＳ３４６）。

【００６８】

このようにして、認証装置２００は、１種類の身体部位だけでなく、複数種類の身体部位による照合を組み合わせることにより、精度の高い本人認証を行うことができる。また、身体部位の種類に応じて、一致度に重み付けをすることで、過去の認証実績に基づいて微妙に判定基準を調整する等の柔軟な本人認証が可能となる。

【００６９】

なお、登録された基準となる特徴データが複数個ある場合には、特徴データごとに、上記照合と認証を繰り返し、少なくとも１つの特徴データについて本人認証が肯定された場合に、最終的に本人認証を肯定し、全ての特徴データについて本人認証が否定された場合に、最終的に本人認証を否定する。

次に、以上のような認証装置２００を備える各種通信装置を操作者が使用しているときの様子を説明する。

【００７０】

図１２は、本人認証のために操作者が携帯電話機５０に対して右手親指の指紋を提示しているときの様子を示す図である。この携帯電話機５０には、ＬＣＤ５３の上方に、バイオメトリック画像を撮影するためのレンズ窓５１と発光窓５２が設けられている。これらレンズ窓５１、発光窓５２及びＬＣＤ５３は、それぞれ、認証装置２００のカメラ部２４０の撮像レンズ２４４、発光部２４８、画像表示部２７０に対応する。

【００７１】

ＬＣＤ５３には、ガイド画像５４と操作者の親指の指紋画像５５とが表示されている。操作者は、固定表示されているガイド画像５４と自分の指紋画像５５の輪郭とがピッタリと一致するように、自分の親指や携帯電話機５０を動かして位置調整する。そして、適切な位置で、指と携帯電話機５０を一定時間（１秒間等

）だけ静止させるか、又は、左手で特定のキーを押すことにより、認証装置２００に指紋画像をキャプチャさせる。キャプチャされた場合には、ＬＣＤ５３上の指紋画像は、しばらくの間（基準輪郭と比較されている間）だけ静止表示される。

【００７２】

図１３は、本人認証のために操作者がＰＤＡ６０に対して右目の虹彩を提示しているときの様子を示す図である。このＰＤＡ６０には、ＬＣＤ６３の上方に、バイオメトリック画像を撮影するためのレンズ窓６１と発光窓６２が設けられている。

操作者は、図１２に示された携帯電話機５０の場合と同様にして、ＬＣＤ６３上に固定表示されているガイド画像６４と自分の虹彩画像６５の輪郭とがピッタリと一致するように、自分の目やＰＤＡ６０を動かして撮影位置を調整する。そして、適正な撮影位置で、指とＰＤＡ６０を一定時間（１秒間等）だけ静止させるか、又は、特定のキーを押すことにより、認証装置２００に虹彩画像をキャプチャさせることができる。

【００７３】

図１４は、本人認証のために操作者がＡＴＭ７０に対して親指の指紋を提示しているときの様子を示す図である。このＡＴＭ７０には、ＣＲＴ７３の上方に、バイオメトリック画像を撮影するためのレンズ窓７１と発光窓７２が設けられている。

このＡＴＭ７０の認証装置２００は、携帯電話機５０やＰＤＡ６０の場合と異なり、カメラ部２４０による被写体の追尾制御を行うことができる。従って、操作者は、一定範囲の適当な位置に親指を静止させているだけでよい。操作者は、レンズ窓７１の動きや、ＣＲＴ７３上のガイド画像７４と虹彩画像７５の輪郭とがピッタリと一致していくように収束する様子を見ることによって、自動位置調整による撮影が行われていることを感じとることができる。

【００７４】

図１５は、ＰＣ８０のＣＲＴ（認証装置２００の画像表示部２７０）の表示例を示す図である。ここには、認証装置２００が有するユーティリティ機能に対応

するメニューが表示されている。

操作者は、このメニューにおいて、「登録」を選択することで、現時点における自分の指紋や虹彩の特徴データを新たに認証サーバ３０又はＩＤカード１１０に登録することができる。ただし、既に特徴データが登録されている場合には、その特徴データによる本人認証に成功した後でなければ登録が拒否される。

【００７５】

また、操作者は、このメニューにおいて、「照合テスト」を選択することで、既に登録されている特徴データをテストする（認証装置２００に現時点での一致度Ｃ１及びＣ２や総合評価値を算出させて表示させる）ことができる。これによって、操作者は、現時点における認証装置２００の認証精度を確認したり、既に登録されている特徴データを更新すべきか否かを判断したりすることができる。

【００７６】

さらに、操作者は、このメニューにおいて、「撮影条件の設定」を選択することで、虹彩に対する撮影条件（ストロボ同期撮影か通常撮影）を選択したり、追尾制御をＯＮ／ＯＦＦしたり、バイオメトリック画像の取得モード（通常モードか高精度モード）を設定したり、繰り返し撮影における繰り返し回数ｎを指定したり、本人認証に使用される身体部位やその組み合わせを指定したりすることができる。

【００７７】

なお、これらユーティリティメニューにおける処理は、認証装置２００の制御部２６０が、入力部２８０及び画像表示部２７０を介して操作者と対話しながら決定していく。そして、決定されたパラメータは、メモリ部２９０や制御部２６０の内部の不揮発メモリ等に格納され、画像取得プログラム２９２ａ等の実行時に用いられる。

【００７８】

以上、本発明に係る認証装置及び電子マネーシステムについて、実施の形態に基づいて説明したが、本発明はこの実施の形態に限られないことは勿論である。

例えば、本発明の本人認証は、通信ネットワーク２０に接続され、認証サーバ３０と通信しながら本人認証を実行する電子マネーシステム１０に用いられたが

、他の様々な用途に適用することができる。

【００７９】

図１６は、本発明に係る本人認証をキーレスの用途に応用した例を示す図である。

図１６（ａ）は、キーレスマンションの入退室管理への適用例を示すイメージ図である。マンションの共同玄関４００に設置された認証装置４０２で取得されたバイオメトリック画像と特徴データは、各戸４１０に設置された認証サーバ機能付きインターフォン４１１に配信される。そして、この認証サーバ機能付きインターフォン４１１によって本人認証が成功した場合に、それと連動した玄関扉４１２のロックが解除される。このようなビル管理システムによって、居住者は、認証サーバ機能付きインターフォン４１１に予めバイオメトリック情報を登録しておくだけで、鍵を持ち歩かなくとも、また、パスワードを忘れてしまっても、ロックアウトされる心配がない。従って、ビルディングの各戸への入退室におけるセキュリティと利便性が増す。

【００８０】

図１６（ｂ）は、キーレス自動車への適用例を示すイメージ図である。この自動車４２０は、キーのロック機構と連動した認証装置４２１を搭載している。認証装置４２１には、この自動車４２０の持主のバイオメトリック情報が予め登録されている。持主は、この認証装置４２１に対して自分の指紋や虹彩を提示し、本人認証に成功してからでないと、キーを差し込んで回転させることができない。つまり、本人認証に成功することによって、初めてエンジンを始動させることができる。これによって、車の盗難が防止される。

【００８１】

図１７は、本発明に係る本人認証を自動販売機に適用した例を示すイメージ図である。この自動販売機４３０は、上記実施の形態における認証装置２００と同等機能の認証装置４３１と、その認証装置４３１により本人認証が成功した場合に、指定された商品を取り出し口に移動させる制御回路等を備える。予め認証サーバにバイオメトリック情報が登録された会員（例えば、この自動販売機４３０が設置されているビル内で働く従業員等）は、専用カードを使用することなく、

又は、専用カードの使用とともに、指紋や虹彩を認証装置４３１に提示することにより、現金を持ち合わせることなく、電子決済によるその場での商品購入をすることができる。

【００８２】

さらに、本発明に係る本人認証をＰＯＳ（Point Of Sales）システムに適用することもできる。例えば、スーパーマーケットにおけるレジスター等のＰＯＳ端末装置に本実施の形態の認証装置２００を装備させ、ＰＯＳシステムにおけるサーバコンピュータに本実施の形態の認証サーバ３０を装備させればよい。これによって、本実施の形態におけるＡＴＭ７０等と同様の入出金処理等が可能となる。つまり、ショッピング等においてパスワードやクレジットカード等が不要になるだけでなく、よりセキュリティの高い本人認証による決済が可能となる。

【００８３】

また、本実施の形態では、バイオメトリック画像を取得する認証装置２００と、特徴データのデータベースを備える認証サーバ３０とは別個独立した装置であったが、これらを一体化させてもよい。これによって、バイオメトリック画像の取得と本人認証とを実行するスタンドアローンの本人認証装置が実現される。

また、本実施の形態の認証装置２００においては、画像処理部２５０がデジタルフィルタ等を用いて特徴データを生成したが、これに代えて、制御部２６０がソフト的に（ＣＰＵに特徴抽出プログラムを実行させることによって）特徴データを生成する構成としてもよい。

【００８４】

また、本実施の形態では、本人認証に用いられるバイオメトリクスの対象は、指紋と虹彩であったが、掌形（手の大きさ、長さ、厚さ、比率等）、顔形（顔の輪郭、目や鼻の形及び配置等）、静脈（手の甲の静脈パターン）、耳介（耳輪や耳甲介腔の大きさ、耳甲介腔幅、耳甲介腔長、形態的耳長等）を加えてもよい。

そして、これら身体部位の中から本人認証に用いるものをユーザが選択してもよい。例えば、認証サーバ３０に登録されたデータベースに基づいて、本人認証に用いることが可能な複数の身体部位をＰＤＡ６０のファンクションキーｆ１～ｆ１０それぞれに割り当てて表示しておき、いずれかのファンクションキーがユ

ーザに押された場合に、そのキーに対応する身体部位を用いた本人認証を実施することとしてもよい。これによって、ユーザの都合に応じた本人認証や、最もセキュリティが高いとユーザが信じる身体部位による本人認証が実現される。

【００８５】

また、本実施の形態では、生体が生きていることを確認するために、瞳孔の動きが検出されたが、これに代えて、黒目の動き、まばたきの有無を検出することとしてもよい。

また、本電子マネーシステム１０における照合においては、特徴データが比較され、バイオメトリック画像そのものは直接的には用いられなかったが、特徴データに代えて、又は、特徴データに加えて、バイオメトリック画像そのものを照合の対象としてもよい。これによって、原画像に基づく本人認証が可能となり、認証サーバ３０やＩＤカード１１０における最新の照合アルゴリズムに基づく精度の高い本人認証が実現される。

【００８６】

【発明の効果】

以上の説明から明らかなように、本発明に係る本人認証装置は、バイオメトリックに基づいて本人認証を行う装置であって、非接触で身体の部位を撮影することによりバイオメトリック画像を取得する撮影手段と、取得されたバイオメトリック画像を表示するバイオメトリック画像表示手段と、適正な撮影位置で前記部位が撮影された場合の部位の外形を示すガイド画像を前記バイオメトリック画像に重ねて表示するガイド表示手段と、前記バイオメトリック画像に基づいて、前記部位が適正な撮影位置で撮影されたか否かを判断する判断手段と、適正な撮影位置で撮影されたと判断された場合に、前記バイオメトリック画像から前記部位の形態的な特徴を示すバイオメトリック情報を抽出し、予め登録されたバイオメトリック情報と照合することにより、本人認証を行う認証手段とを備えることを特徴とする。

【００８７】

これによって、非接触でバイオメトリック画像が採取され、本人認証が行われるので、接触センシングに起因する従来の不具合は解消される。そして、画像表

示手段にはバイオメトリック画像だけでなく、適正な撮影位置を示すガイド画像も同時に表示されるので、操作者は、それら画像が重なるように身体部位を移動させることにより、ピントの合った鮮明なバイオメトリック画像に基づく本人認証を行うことができる。

【００８８】

ここで、前記本人認証装置は、さらに、適正な撮影位置で前記部位が撮影されるように前記撮影手段による撮影の方向と倍率とを制御する撮影制御手段を備えてもよい。これによって、操作者は、本人認証に用いる身体部位を適当な空間位置で静止させているだけで、本人認証装置の追尾制御による自動撮影が行われる。

【００８９】

また、前記本人認証装置は、さらに、前記部位又は前記部位を含むより大きな部位を繰り返して撮影するように前記撮影手段を制御し、得られた複数の画像に基づいて、身体の動きを検出する動き検出手段を備え、前記認証手段は、前記動き検出手段によって身体の動きが検出され、かつ、前記部位が適正な撮影位置で撮影されたと判断された場合に、本人認証を行ってもよい。これによって、動きが確認された身体部位による本人認証、即ち、生きた生体による本人認証が行われ、死体を用いた不正な本人認証が防止される。

【００９０】

また、前記部位は、虹彩であり、前記動き検出手段は、前記虹彩に光を照射するとともに、その照射に同期して虹彩を撮影するように前記撮影手段を制御してもよい。これによって、瞳孔が萎んだ状態での虹彩、即ち、より面積の大きい状態での虹彩による本人認証が行われ、認証精度が向上される。また、光に対する瞳孔の反応（拡大・収縮）の有無を検出することで、生体が生きているか否かを確認することも可能となる

また、前記本人認証装置は、さらに、繰り返して前記部位を撮影するように前記撮影手段を制御する繰り返し制御手段を備え、前記認証手段は、繰り返し撮影によって得られた複数のバイオメトリック画像に基づいて前記バイオメトリック情報を抽出し、本人認証を行ってもよい。これによって、身体部位の動きを検出

することが可能となるので、生体が生きていることを確認した後に本人認証を行うことができる。

【００９１】

また、前記本人認証装置は、さらに、身体の複数の部位について、前記バイオメトリック画像を取得し、取得されたバイオメトリック画像を表示し、前記ガイド画像を表示し、前記部位が適正な撮影位置で撮影されたか否かを判断するように前記撮影手段と、前記バイオメトリック画像表示手段と、前記ガイド表示手段と、判断手段とを制御する複数部位制御手段を備え、前記認証手段は、取得された複数の部位のバイオメトリック画像から複数の部位についてのバイオメトリック情報を抽出し、それらバイオメトリック情報の組み合わせと予め登録された対応するバイオメトリック情報の組み合わせとを照合することにより、本人認証を行ってもよい。例えば、指紋と虹彩の組み合わせとしてもよい。

【００９２】

これによって、１種類の身体部位だけによる本人認証よりも高い精度で認証が行われる。また、同一の撮影手段により、複数の身体部位に基づく本人認証が行われるので、２以上の種類のセンサを組み合わせて本人認証する場合に比べ、低コストとなる。

また、前記認証手段は、前記複数の部位ごとの照合結果を示す一致度それぞれに異なる重みづけをした後に加算して得られる総合評価値が一定のしきい値を超えるか否かによって、前記本人認証を行ってもよい。これによって、身体部位の種類に応じた重み付けができるので、きめの細かい高精度な本人認証が実現される。

【００９３】

また、前記複数の部位は、異なる指の指紋としたり、両目の虹彩としてもよい。これによって、ほぼ同じ撮影位置で複数の身体部位による本人認証が可能となり、撮影条件の変更が少なくて済む。

また、前記本人認証装置は、さらに、前記撮影に伴って、本人の識別に役立つ情報であるＩＤデータを取得するＩＤデータ取得手段を備え、前記認証装置は、前記バイオメトリック情報及び前記ＩＤデータの組み合わせと予め登録されたバ

イオメトリック情報及びＩＤデータの組み合わせとを照合することにより、本人認証を行ってもよい。これによって、本人認証の精度が向上される。

【００９４】

また、前記認証手段は、予め登録された複数のバイオメトリック情報の中から、ＩＤデータが一致するものを特定し、特定したバイオメトリック情報と抽出された前記バイオメトリック情報との同一性によって、本人認証を行ってもよい。これによって、バイオメトリック情報による照合に先立って、ＩＤデータを用いた検索対象の絞り込みが行われるので、本人認証に要する処理時間が削減される。

【００９５】

また、前記認証装置は、さらに、予め登録された前記バイオメトリック情報を記憶する記憶手段と、前記記憶手段に記憶されたバイオメトリック情報を前記認証手段により抽出されたバイオメトリック情報で置き換える登録情報更新手段を備えてもよい。これによって、更新可能なデータベース（登録されたバイオメトリック情報群）を備えるスタンドアローンタイプの本人認証装置が実現される。

【００９６】

また、前記更新手段は、予め定められた一定期間を超えてバイオメトリック情報が更新されていない場合に、前記バイオメトリック情報を置き換えてもよい。これによって、登録データベースは最新のものに維持されるので、高い精度による本人認証が継続される。

以上のように、本発明は、ユーザに心理的な不快感や嫌悪感を与えることのない非接触センシングによる低コストで、かつ、複数のバイオメトリック画像に基づく高い精度の本人認証を行うことができ、その実用的価値は極めて高い。

【図面の簡単な説明】

【図１】

本発明に係る電子マネーシステムの全体構成を示す図である。

【図２】

同システムにおける認証サーバに備えられているデータベースの内容を示す図である。

【図３】

（ａ）は、ＩＤデータだけが記録された最も簡易なタイプ１のＩＤカード、

（ｂ）は、さらに特徴データが記録されたタイプ２のＩＤカード、

（ｃ）は、さらに認証回路を備える最も高機能なタイプ３のＩＤカードの概観図である。

【図４】

同システムのＡＴＭ等が備える認証装置の構成を示すブロック図である。

【図５】

同認証装置のカメラ部の詳細な構成を示すブロック図である。

【図６】

同認証装置の画像処理部が生成する指紋の特徴データを説明するための図である。

【図７】

同認証装置の画像処理部が生成する虹彩の特徴データを説明するための図である。

【図８】

通常モードにより認証装置がバイオメトリック画像を取得する場合の動作手順を示すフローチャートである。

【図９】

高精度モードにより認証装置がバイオメトリック画像を取得する場合の動作手順を示すフローチャートである。

【図１０】

同認証装置による特徴データの照合における全体的の流れを示すフローチャートである。

【図１１】

図１０における照合及び認証処理の詳細な手順を示すフローチャートである。

【図１２】

同認証装置を備える携帯電話機を用いて操作者が本人認証をしている様子を示す図である。

【図１３】

同認証装置を備えるＰＤＡを用いて操作者が本人認証をしている様子を示す図である。

【図１４】

同認証装置を備えるＡＴＭを用いて操作者が本人認証をしている様子を示す図である。

【図１５】

同認証装置が有するユーティリティ機能に対応するメニューの表示例である。

【図１６】

（ａ）は、同認証装置をキーレスマンションの入退室管理に適用した例を示すイメージ図であり、

（ｂ）は、キーレス自動車に適用した例を示すイメージ図である。

【図１７】

同認証装置を自動販売機に適用した例を示すイメージ図である。

【図１８】

従来の認証装置が備えるバイオメトリックセンサの例を示し、

（ａ）は、光学式指紋スキャナと呼ばれる方式、

（ｂ）は、静電容量型指紋センサチップによる方式を示す図である。

【符号の説明】

１０　電子マネーシステム

２０　通信ネットワーク

３０　認証サーバ

４０　ゲートウェイ

５０　携帯電話機

６０　ＰＤＡ

７０　ＡＴＭ

８０　ＰＣ

９０　銀行用通信端末

１００　電子ショップ用通信端末

１１０　ＩＤカード
２００　認証装置
２１０　撮影条件切替部
２２０　リーダライタ部
２３０　通信Ｉ／Ｆ部
２４０　カメラ部
２４１　可動部
２４２　駆動部
２４３　Ｚ駆動部
２４４　撮像レンズ
２４５　イメージセンサ部
２４６　ＡＦ制御部
２４７　キャプチャ制御部
２４８　発光部
２５０　画像処理部
２６０　制御部
２７０　画像表示部
２８０　入力部
２８５　暗号部
２９０　メモリ部
２９１　基準データ格納部
２９２　プログラム格納部
２９３　一時データ格納部
４００　共同玄関
４０２　認証装置
４１０　各室内
４１１　認証サーバ機能付きインターフォン
４１２　玄関扉
４２０　自動車

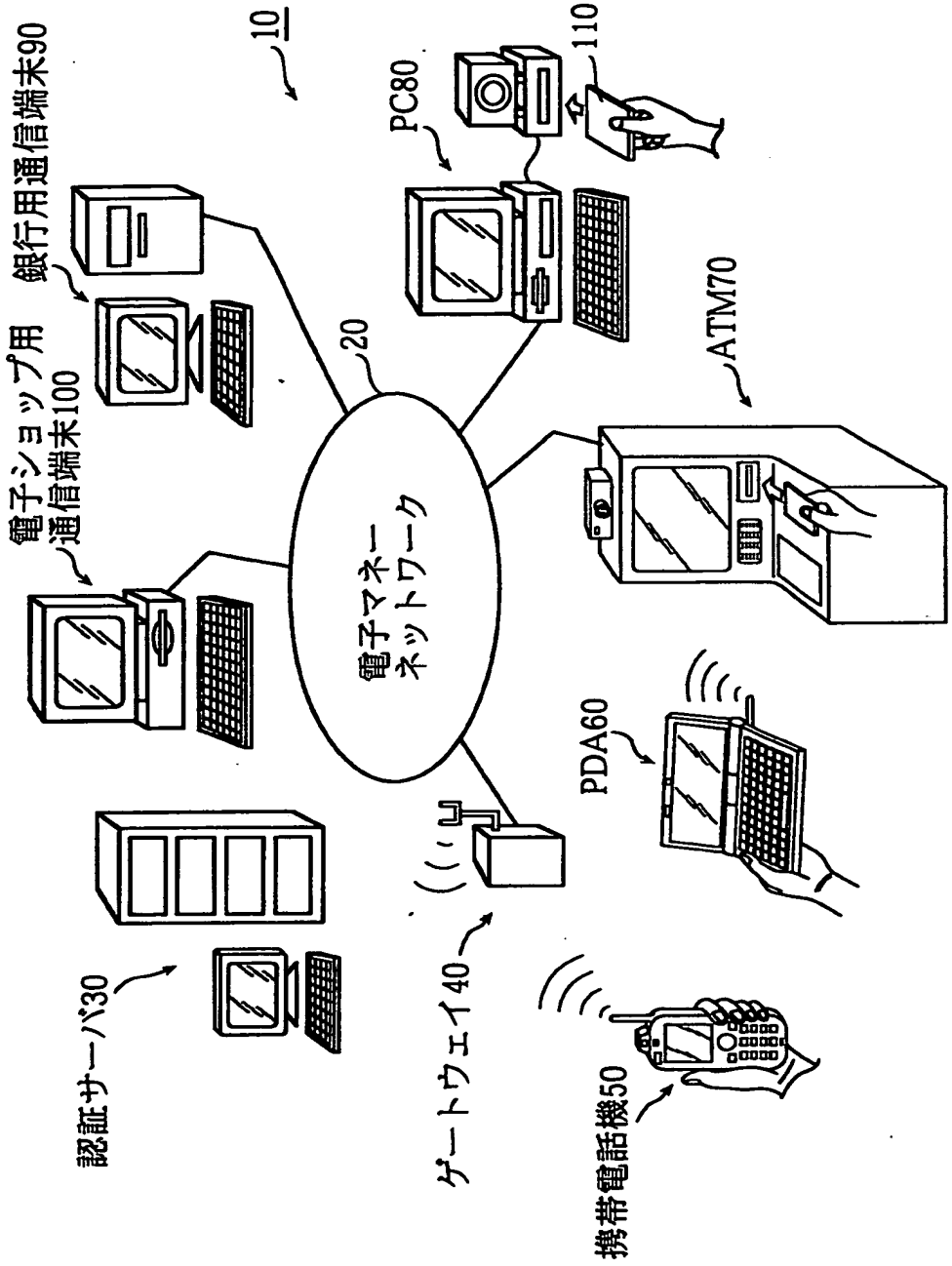
４２１　　認証装置

４３０　　自動販売機

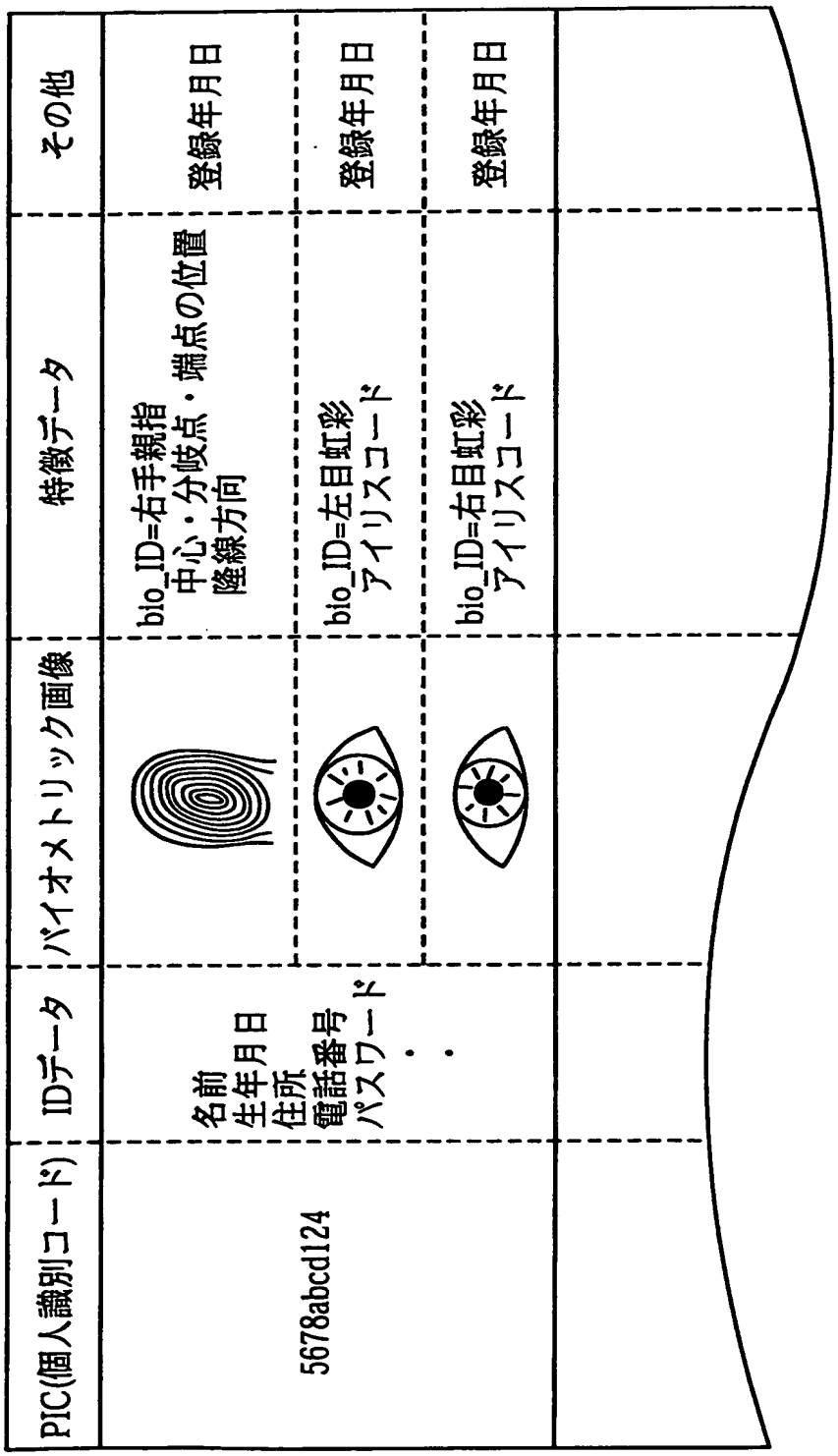
４３１　　認証装置

【書類名】　　図面

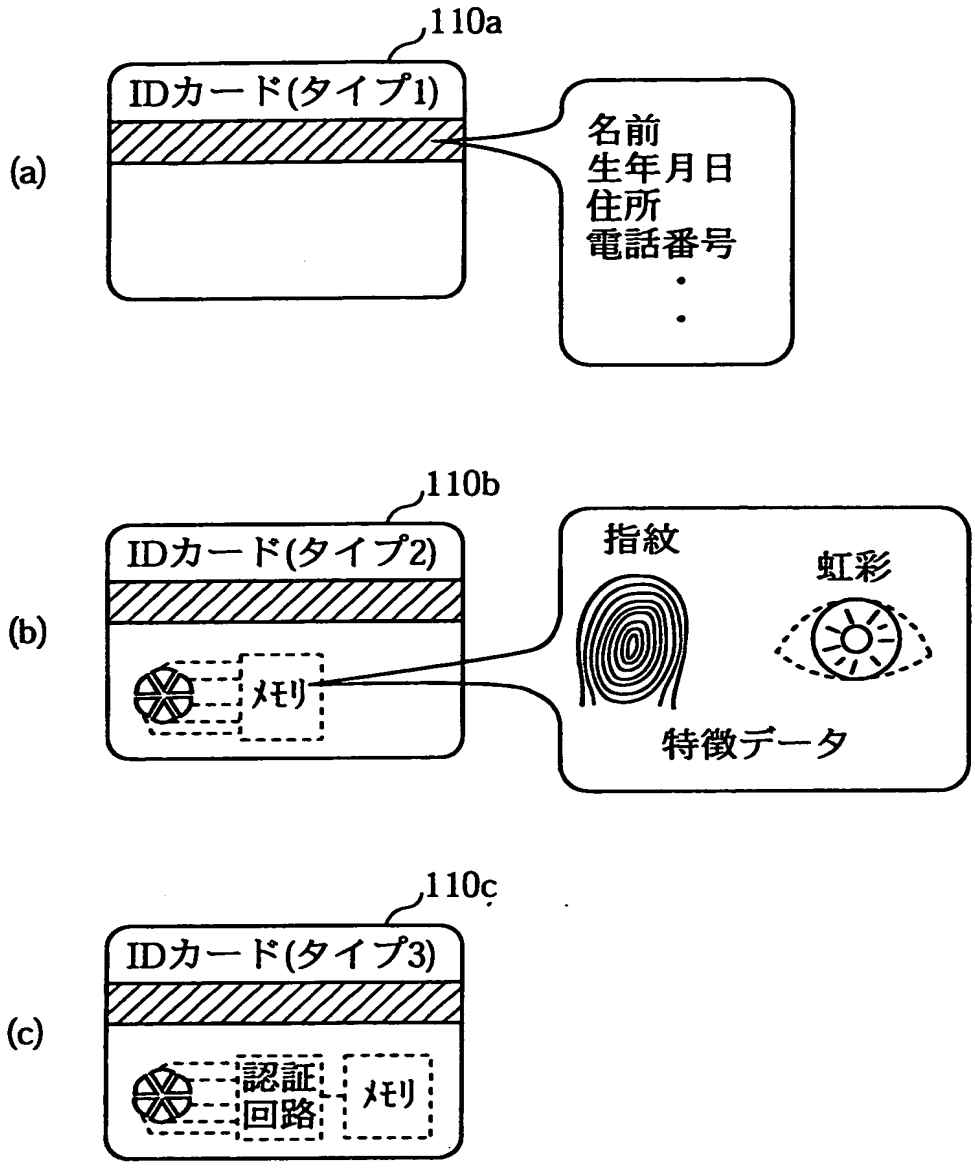
【図１】


10
銀行用通信端末90
電子ショップ用
通信端末100
PC80
110
20
ATM70
電子マネー
ネットワーク
PDA60
認証サーバ30
ゲートウェイ40
携帯電話機50

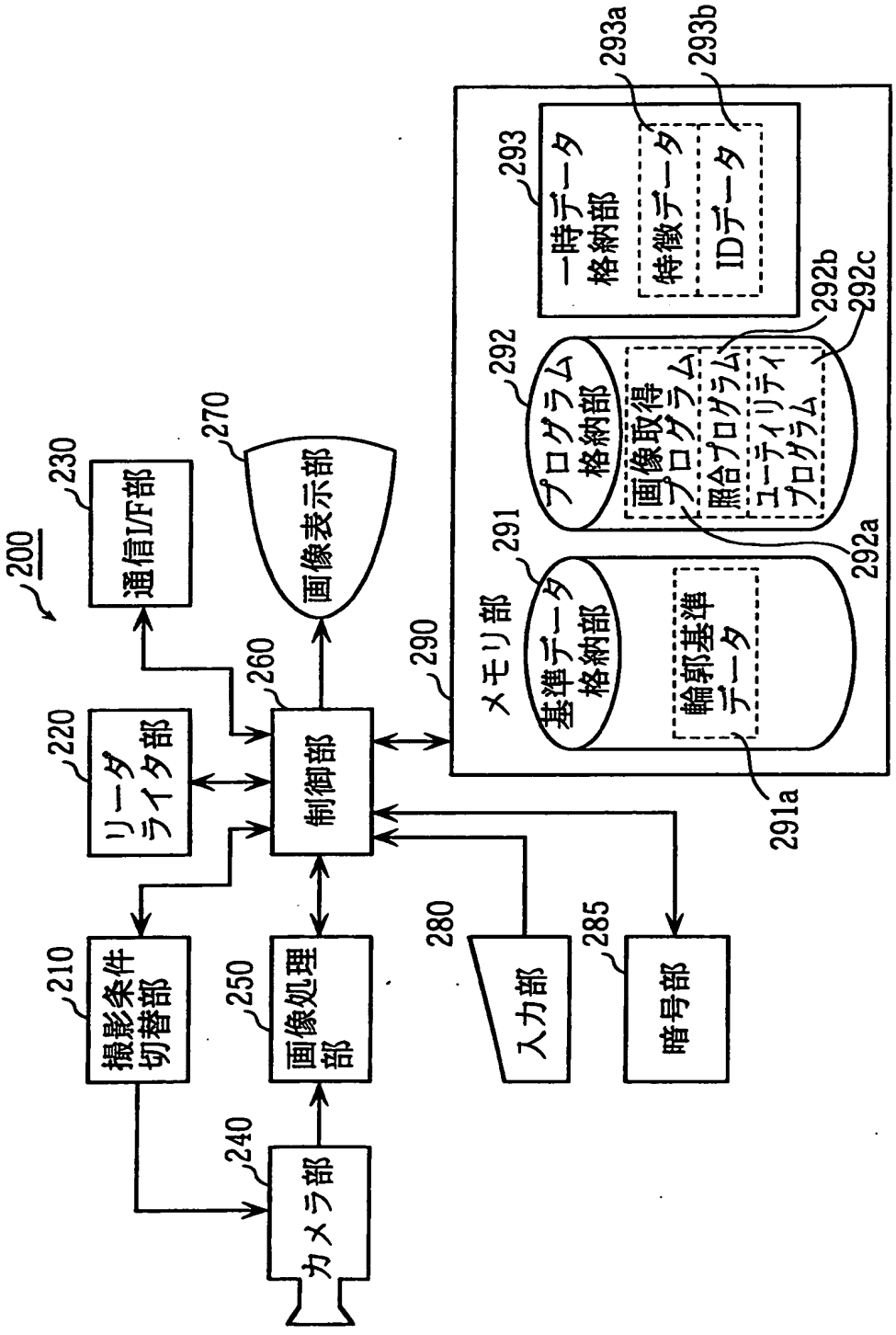
【図２】


PIC(個人識別コード)
IDデータ
バイオメトリック画像
特徴データ
その他
5678abcd124
名前
生年月日
住所
電話番号
パスワード
・
・
bio_ID=右手親指
中心・分岐点・端点の位置
隆線方向
登録年月日
bio_ID=左目虹彩
アイリスコード
登録年月日
bio_ID=右目虹彩
アイリスコード
登録年月日

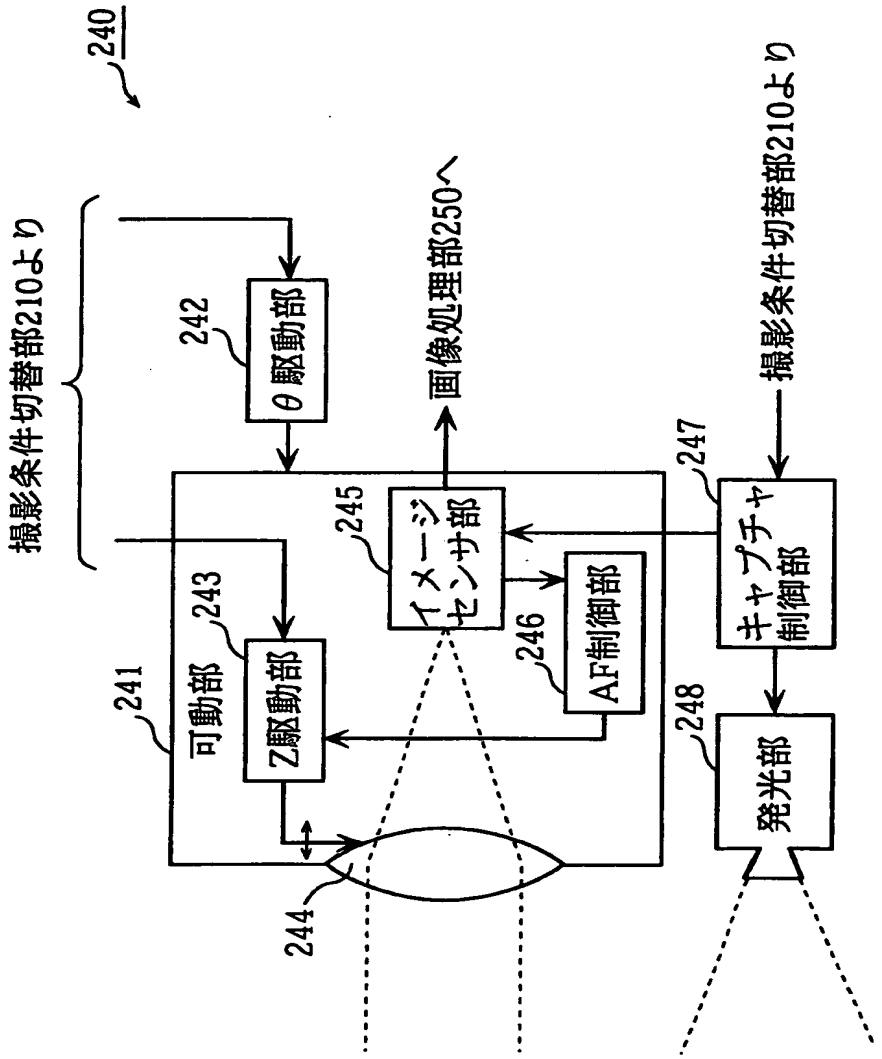
【図３】


110a
IDカード(タイプ1)
(a)
名前
生年月日
住所
電話番号
110b
IDカード(タイプ2)
(b)
メモリ
指紋
虹彩
特徴データ
110c
IDカード(タイプ3)
(c)
認証
回路
メモリ

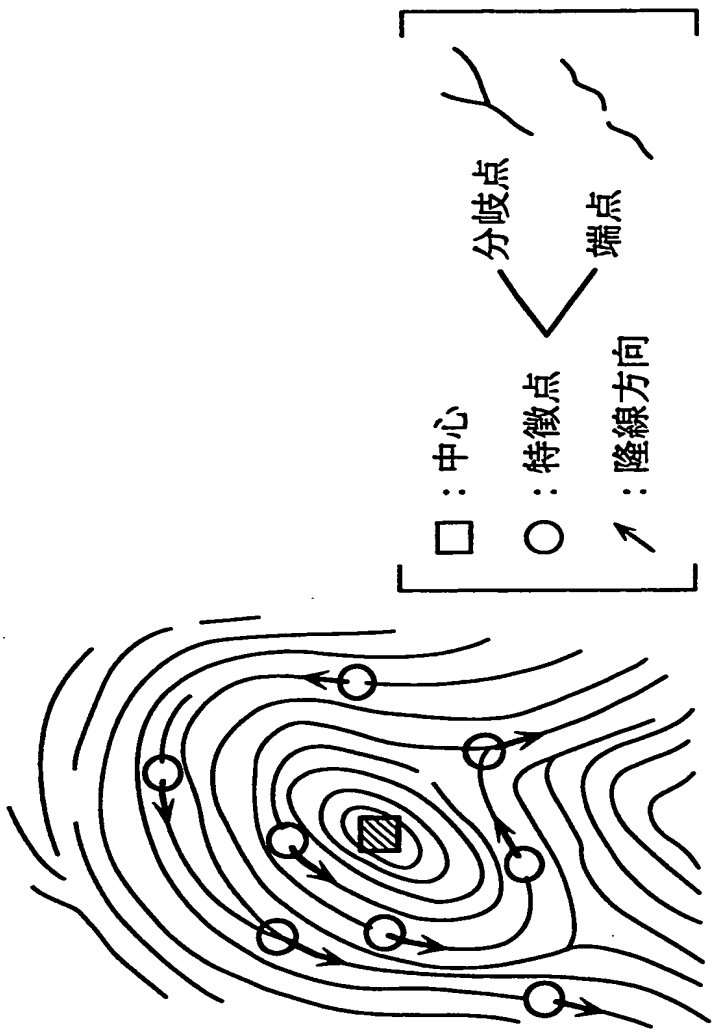
【図４】


200
通信I/F部
230
画像表示部
270
リーダライタ部
220
制御部
260
290
メモリ部
291
基準データ格納部
輪郭基準データ
291a
292
プログラム格納部
画像取得プログラム
照合プログラム
ユーティリティプログラム
292a
292b
292c
293
一時データ格納部
特徴データ
IDデータ
293a
293b
撮影条件切替部
210
画像処理部
250
カメラ部
240
入力部
280
暗号部
285

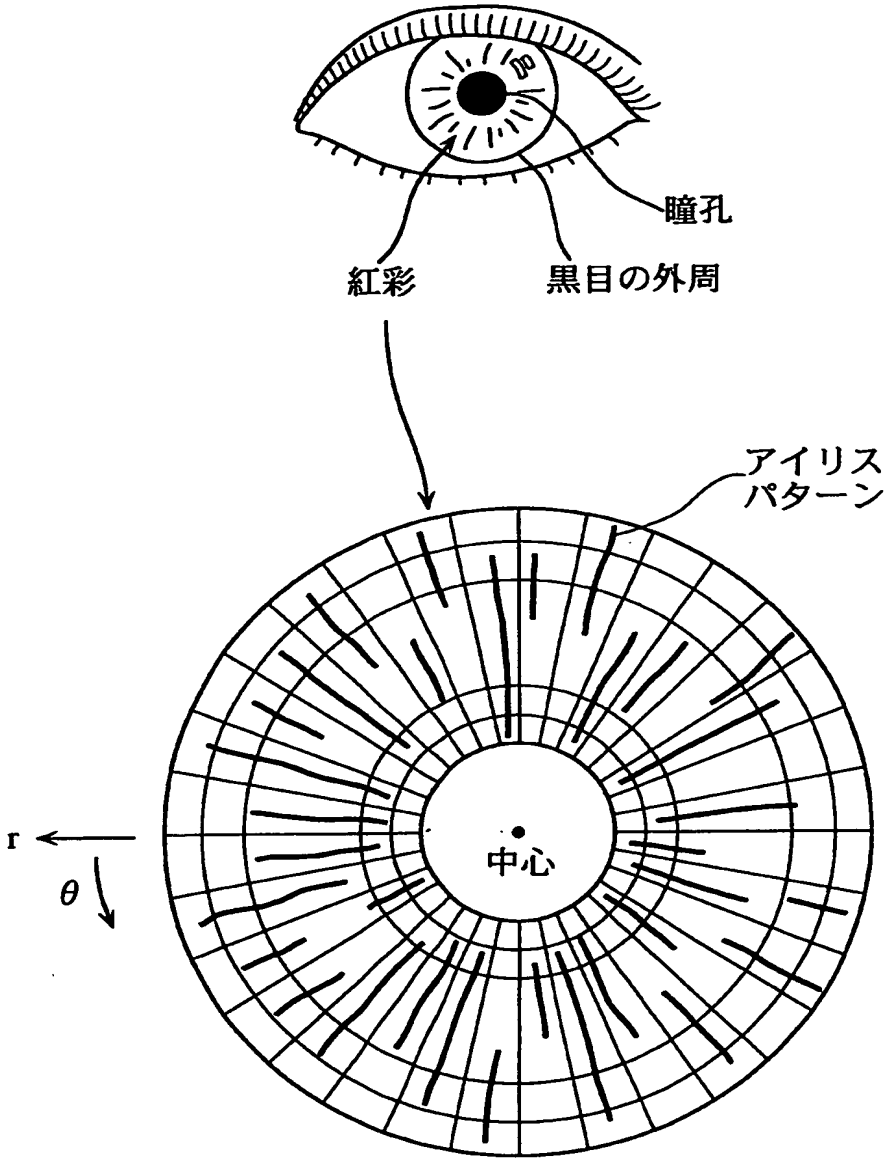
【図５】


240
撮影条件切替部210より
242
θ駆動部
画像処理部250へ
撮影条件切替部210より
247
245
イメージセンサ部
キャプチャ制御部
243
Z駆動部
246
AF制御部
241
可動部
248
発光部
244

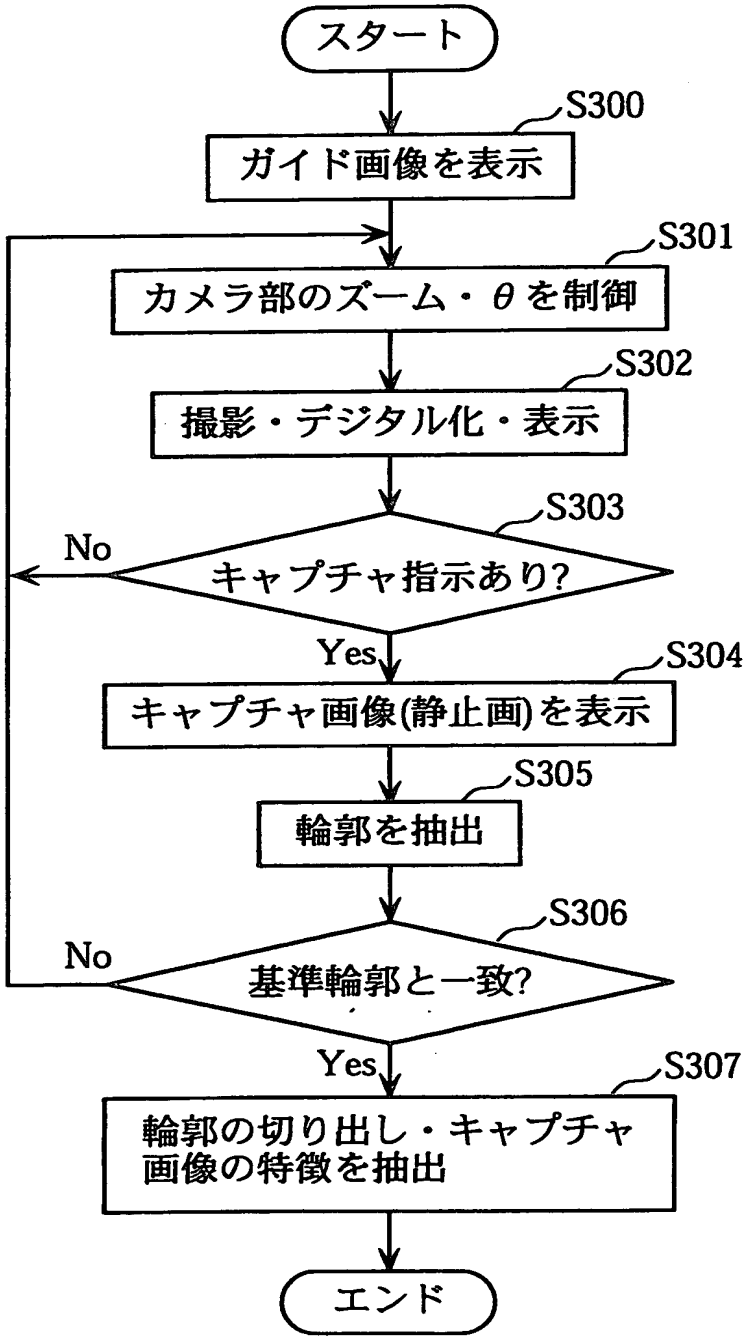
【図６】



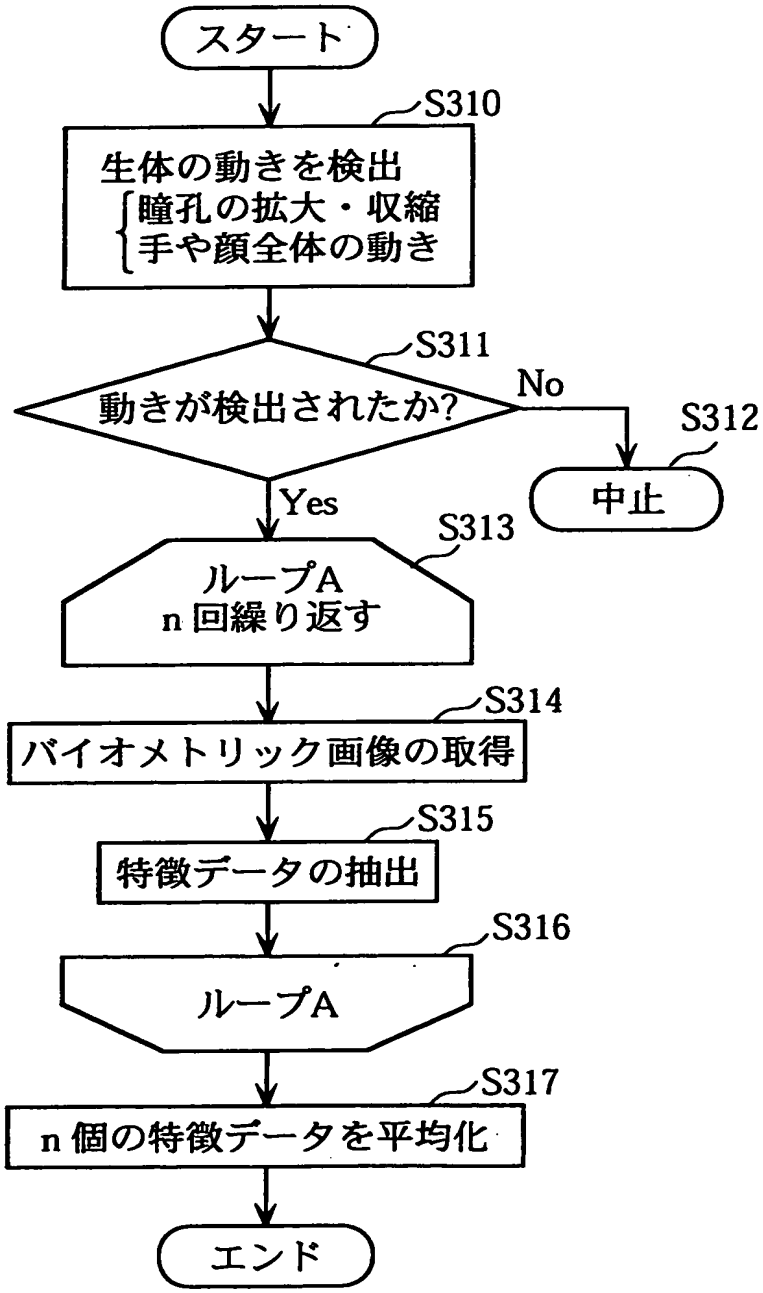
【図７】



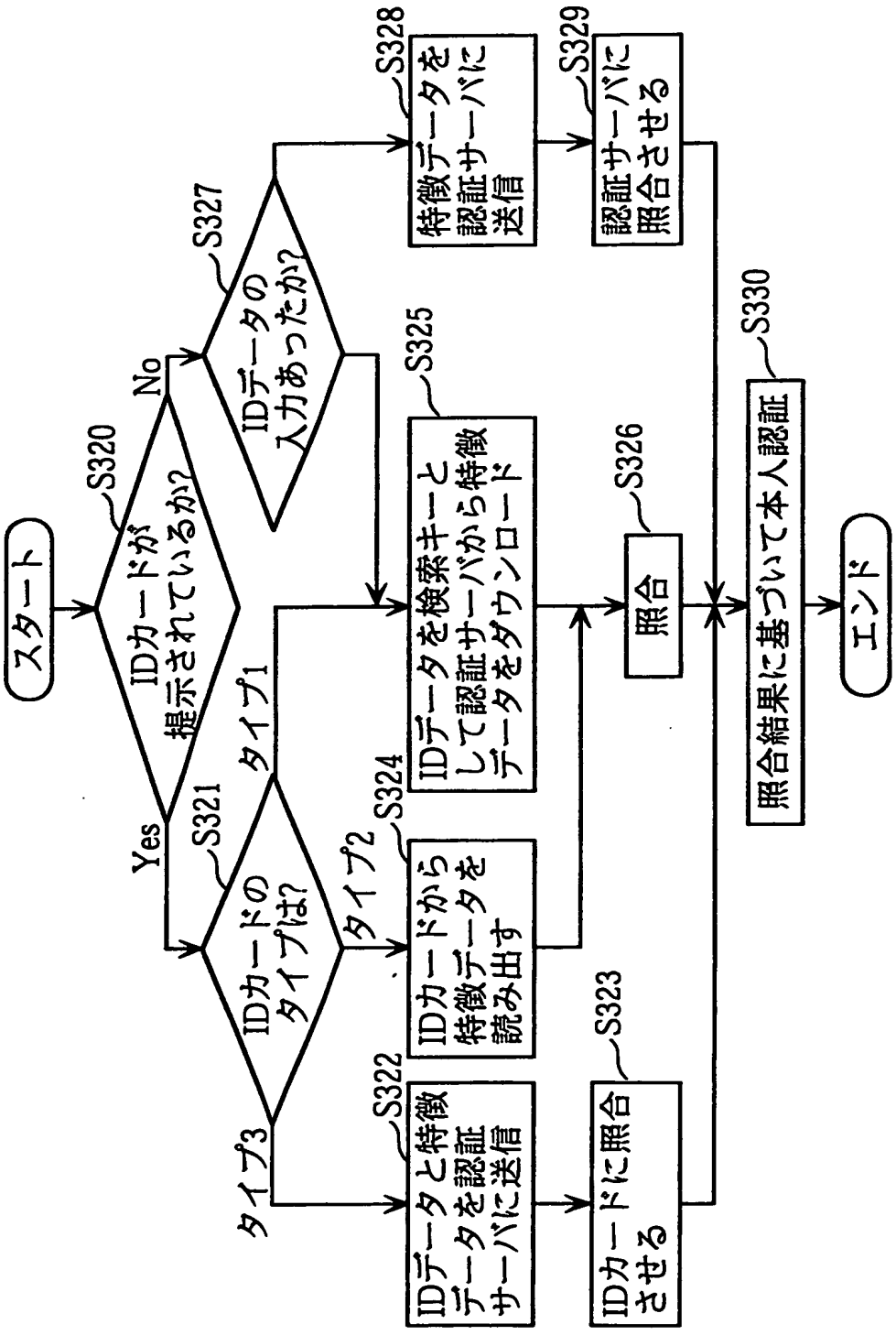
【図８】


スタート
S300
ガイド画像を表示
S301
カメラ部のズーム・θを制御
S302
撮影・デジタル化・表示
S303
No
キャプチャ指示あり?
Yes
S304
キャプチャ画像(静止画)を表示
S305
輪郭を抽出
S306
No
基準輪郭と一致?
Yes
S307
輪郭の切り出し・キャプチャ画像の特徴を抽出
エンド

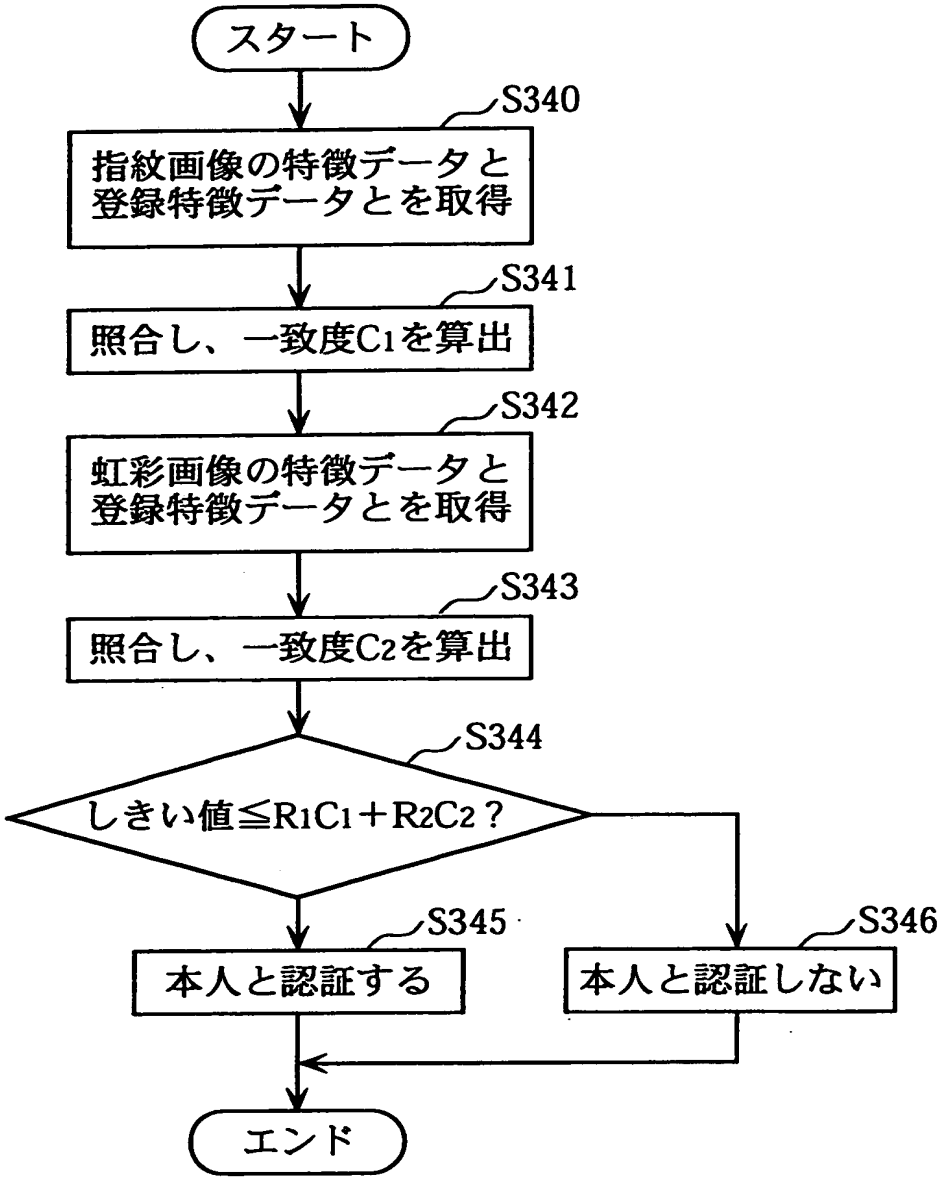
【図９】


スタート
S310
生体の動きを検出
瞳孔の拡大・収縮
手や顔全体の動き
S311
動きが検出されたか?
No
S312
中止
Yes
S313
ループA
n 回繰り返す
S314
バイオメトリック画像の取得
S315
特徴データの抽出
S316
ループA
S317
n 個の特徴データを平均化
エンド

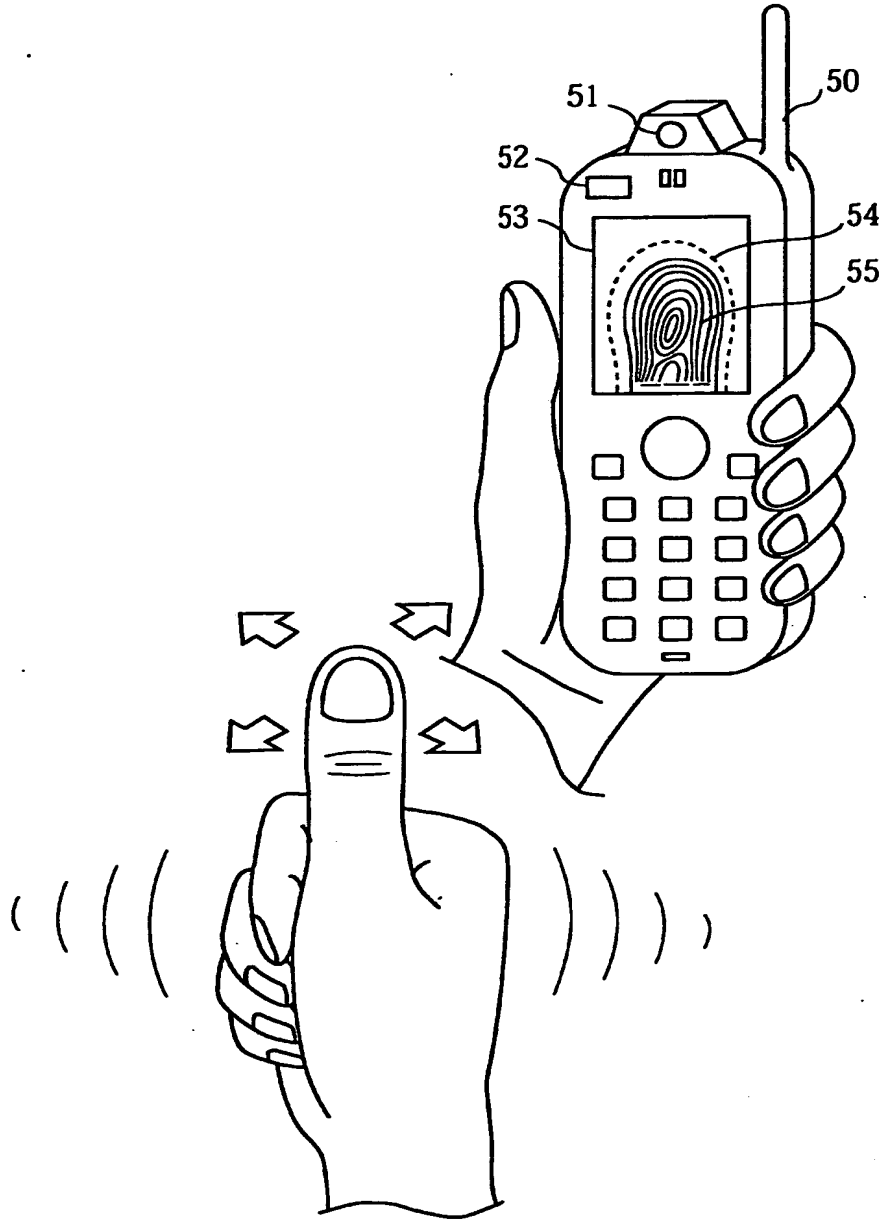
【図１０】


スタート
S320
IDカードが提示されているか?
No
Yes
S321
IDカードのタイプは?
タイプ1
タイプ2
タイプ3
S322
IDデータと特徴データを認証サーバに送信
S323
IDカードに照合させる
S324
IDカードから特徴データを読み出す
S325
IDデータを検索キーとして認証サーバから特徴データをダウンロード
S326
照合
S327
IDデータの入力あったか?
S328
特徴データを認証サーバに送信
S329
認証サーバに照合させる
S330
照合結果に基づいて本人認証
エンド

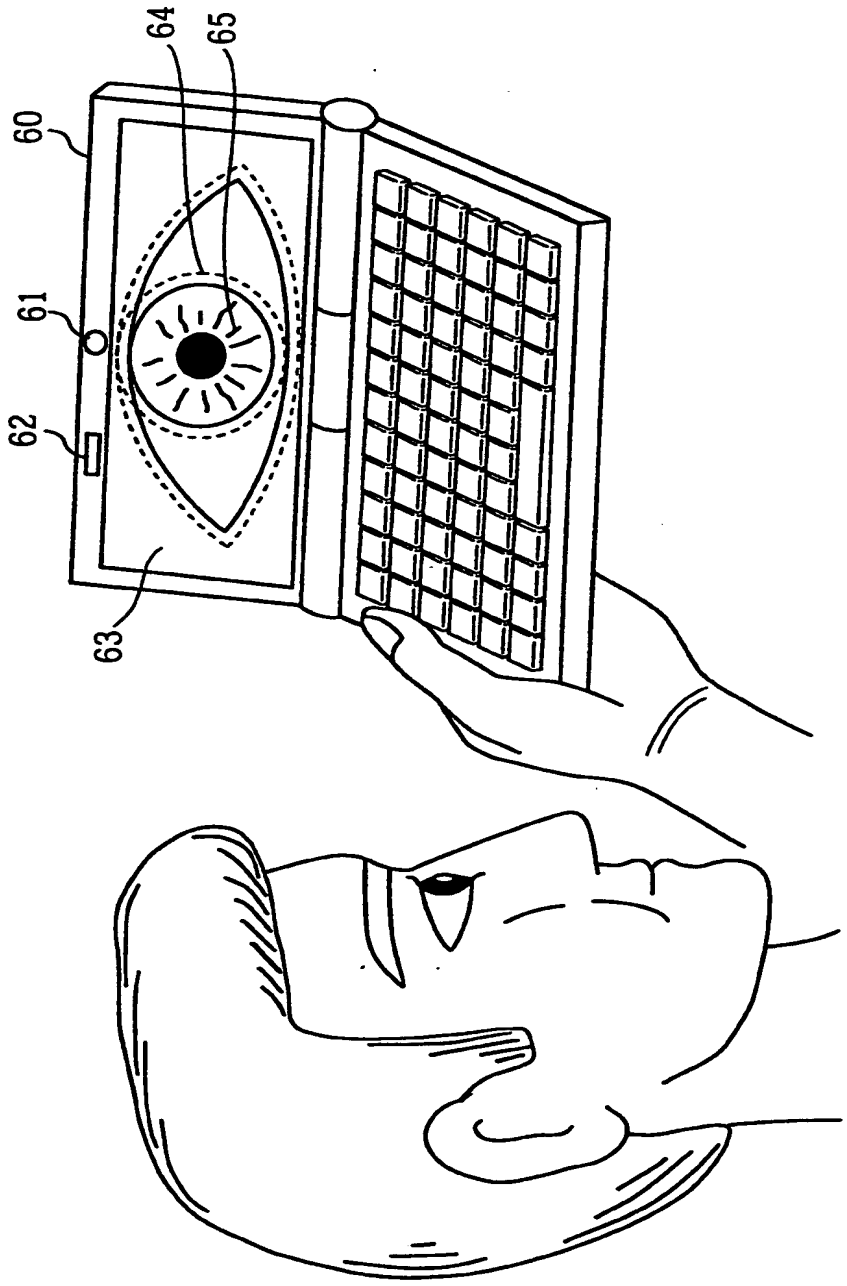
【図１１】


スタート
S340
指紋画像の特徴データと
登録特徴データとを取得
S341
照合し、一致度C1を算出
S342
虹彩画像の特徴データと
登録特徴データとを取得
S343
照合し、一致度C2を算出
S344
しきい値≦R1C1＋R2C2？
S345
本人と認証する
S346
本人と認証しない
エンド

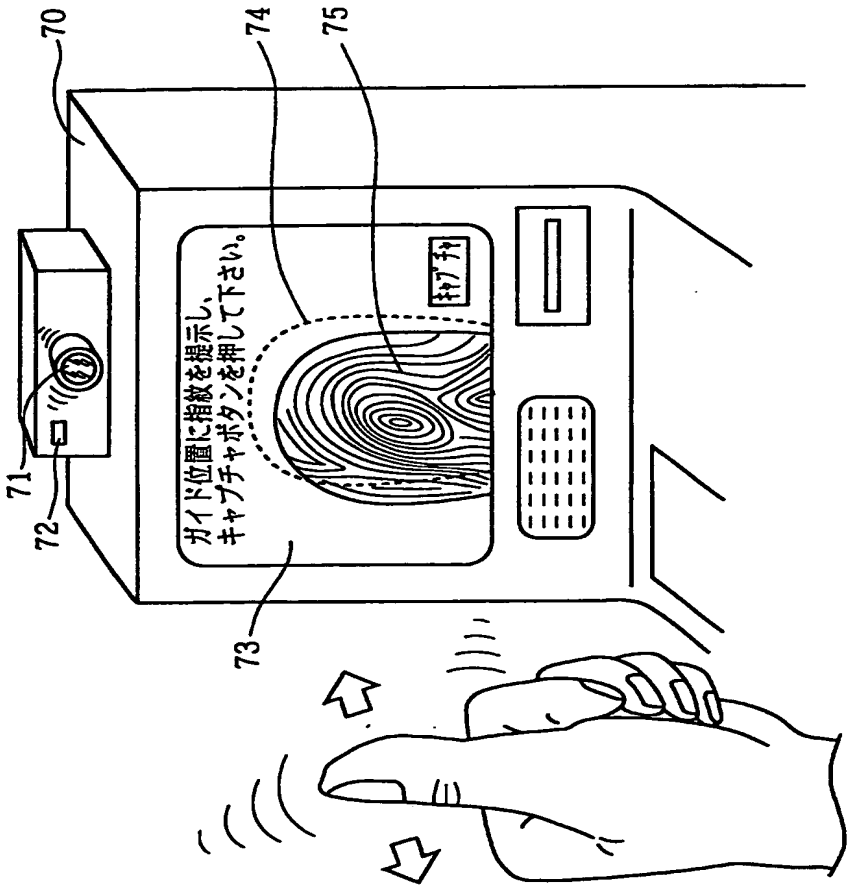
【図１２】



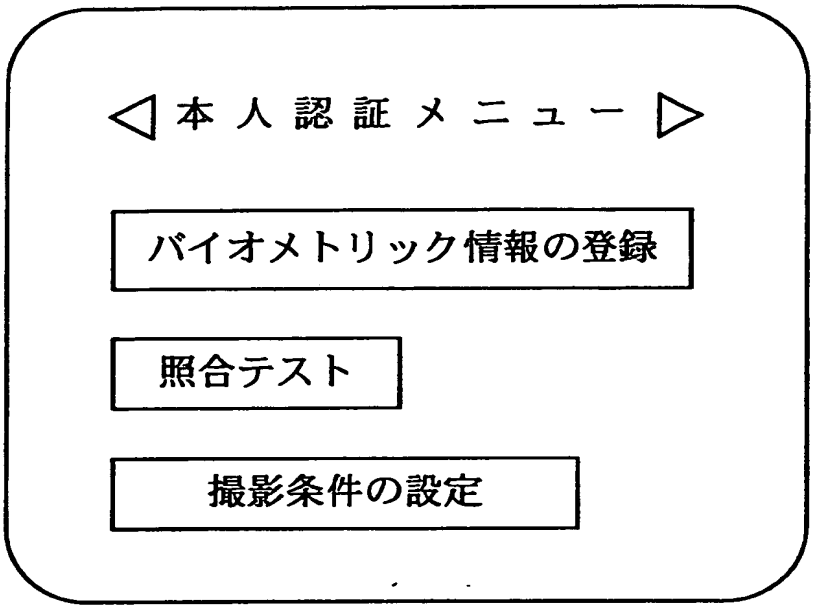
【図１３】



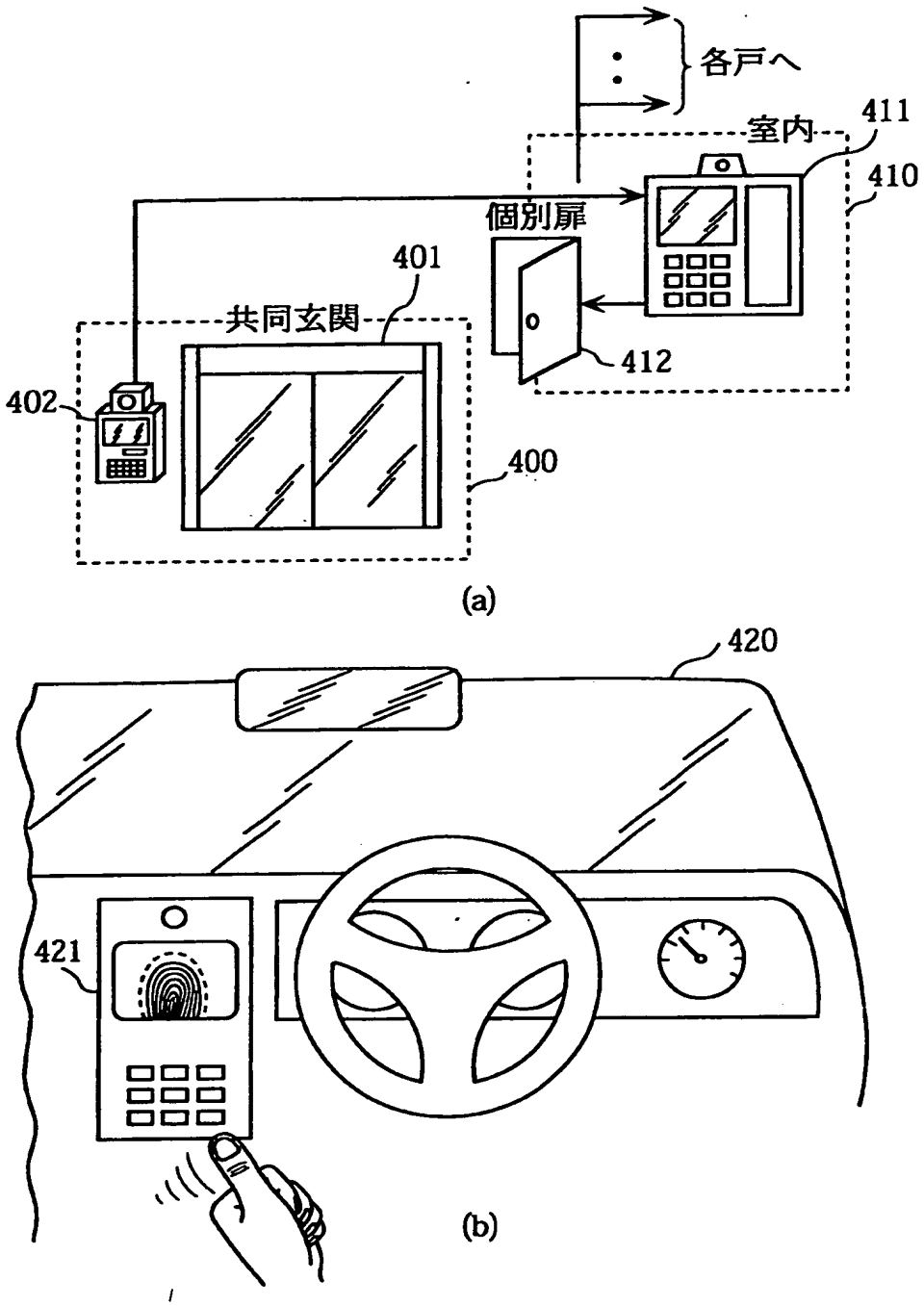
【図１４】



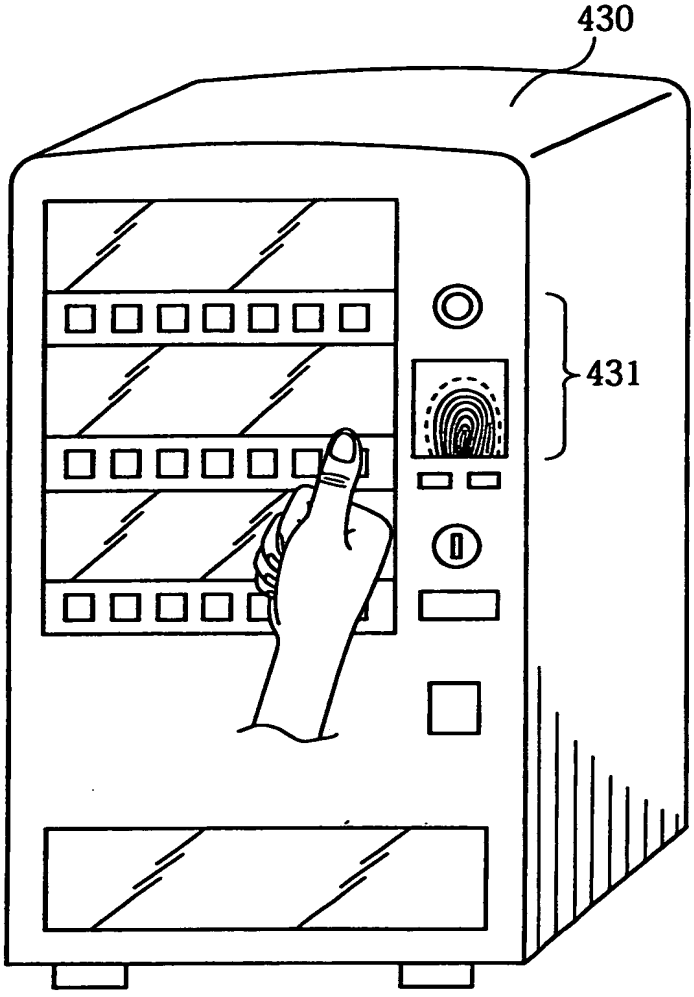
【図１５】



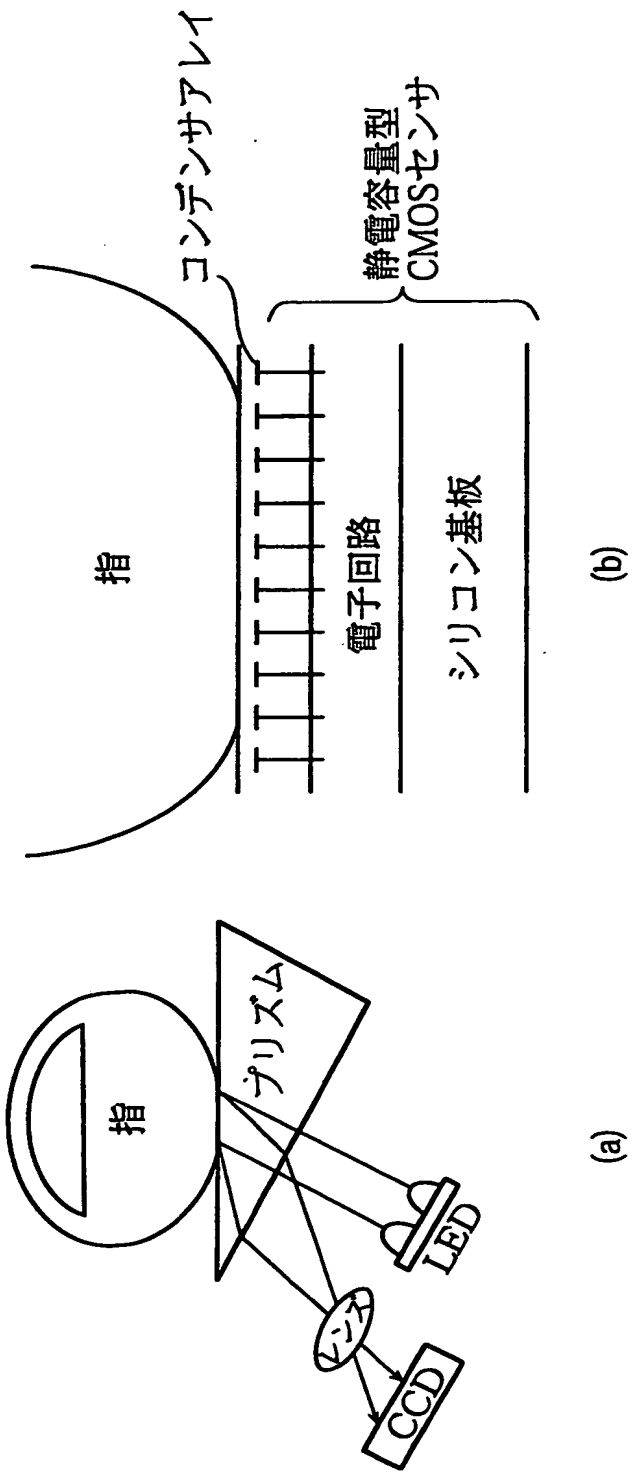
【図１６】



【図１７】



【図１８】



【書類名】　　要約書

【要約】

【課題】　ユーザに心理的な不快感や嫌悪感を与えることなく、精度の高い本人認証を行う認証装置を提供する。

【解決手段】　非接触で身体の部位（指紋及び虹彩等）を撮影することによりバイオメトリック画像を取得するカメラ部２４０及び画像処理部２５０と、その部位を最適な撮影位置に誘導するためのガイド画像とバイオメトリック画像とを重ねて表示するための画像表示部２７０と、取得されたバイオメトリック画像から特徴データを抽出し、暗号部２８５に暗号化させた後に認証サーバ３０に送信する制御部２６０及び通信Ｉ／Ｆ部２３０等を備える。

【選択図】　　図４

出 願 人 履 歴 情 報

識別番号　　〔０００００５８４３〕

１．変更年月日　　１９９３年　９月　１日
［変更理由］　住所変更
住　所　大阪府高槻市幸町１番１号
氏　名　松下電子工業株式会社